[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷
H04N 7/16
H04N 7/167

[12]发明专利申请公开说明书

[21]申请号 02105403.7

[43]公开日 2002年10月9日

[11]公开号 CN 1373609A

[22]申请日 2002.2.9 [21]申请号 02105403.7

[30]优先权

[32]2001.2.9 [33]JP [31]034057/2001

[32]2001.2.16 [33]JP [31]040787/2001

[71]申请人 佳能株式会社

地址 日本东京

[72]发明人 林淳一

[74]专利代理机构 中国国际贸易促进委员会专利商标事务所

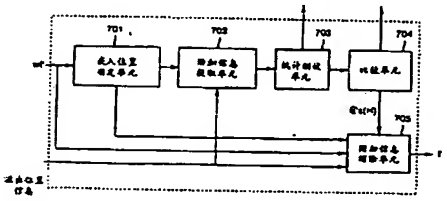
代理人 付建军

权利要求书5页 说明书27页 附图页数21页

[54]发明名称 信息处理装置及其控制方法、计算机程序和存储介质

[57]摘要

依据本发明，当鉴别信息从数字信息以不可分割的方式设置时，总能检测 到信息是否被干扰，而且只要数字数据没受干扰，就能将其恢复。为了实现这个目的，当将鉴别信息嵌入到由图像输入单元(201)输入的数 字信息时，散列值计算单元(202)产生基于该数字信息的鉴别信息，加密单元 (203)使用加秘密钥对鉴别信息加密，以及数字水印形成单元(204)将加密 的信息作为数字水印嵌入到数字信息。



ISSN1008-4274

权 利 要 求 书

1. 一种用于将鉴别信息嵌入数字信息的信息处理装置，包括：

用于产生鉴别信息的装置，用于在将要把鉴别信息嵌入到其中的数字信息的基础上产生该鉴别信息；和

数字水印形成装置，用于将所产生的鉴别信息嵌入到数字信息中并使数字信息。

2. 根据权利要求 1 的装置，其中所述的鉴别信息为数字签名。

3. 根据权利要求 1 的装置，进一步包括使用私人密钥给数字信息加密的加密装置，并且其中数字签名为使用私人密钥给数字信息加密而获得的数据。

4. 根据权利要求 1 的装置，进一步包括用于计算数字信息散列值的散列值计算装置，和使用私人密钥给散列值加密的加密装置，其中数字签名为使用私人密钥给散列值加密而获得的数据。

5. 根据权利要求 1 的装置，其中的鉴别信息为 MAC。

6. 根据权利要求 5 的装置，进一步包括用于计算数字信息散列值的散列值计算装置，和使用私人密钥对散列值进行算术运算的算术运算装置，其中 MAC 为使用私人密钥对数字信息的散列值进行算术运算而获得的数据。

7. 根据权利要求 2 的装置，其中的鉴别信息除了包括有数字签名之外，还至少包括日期信息、位置信息、时间信息、装置的独特信息和签名人的专有信息中的一种。

8. 一种用于鉴别数字信息的信息处理装置，其中的鉴别信息是作为数字水印而嵌入到数字信息的，该装置包括：

用于从数字信息中提取出作为数字水印而被嵌入的鉴别信息作为第一鉴别信息的装置；

数字水印消除装置，用于消除从数字信息中提取出的作为数字水印的鉴别信息，并恢复推测的原始数字信息；

生成装置，依据由所述数字水印消除装置消除数字水印而恢复的推测的原始数字信息产生一个第二鉴别信息；和

用于将第一鉴别信息与第二鉴别信息进行比较的比较装置。

9. 根据权利要求 8 的装置，进一步包括通知装置，在第一鉴别信息与第二

鉴别信息互等时，通知输入的数字信息没有受到干扰，而在第一鉴别信息与第二鉴别信息互不相等时，通知输入的数字信息受到了干扰。

10. 根据权利要求 8 的装置，其中所述的鉴别信息为数字签名。

11. 根据权利要求 8 的装置，进一步包括使用私人密钥对数字签名进行加密的加密装置，其中比较单元把由解密第二鉴别信息而得到的信息与第一鉴别信息进行比较。

12. 根据权利要求 8 的装置，进一步包括用于计算其中消除了数字水印的数字信息的散列值的散列值计算装置，和使用公共密钥对数字签名进行解密的解密装置，其中比较装置将使用公共密钥解密第二鉴别信息而得到的信息与散列值进行比较。

13. 根据权利要求 8 的装置，其中的鉴别信息为 MAC。

14. 根据权利要求 12 的装置，进一步包括用于计算其中消除了数字水印的数字信息的散列值计算装置和使用私人密钥对 MAC 进行算术运算的算术运算装置，其中比较装置将使用私人密钥解密 MAC 而得到的信息与散列值进行比较。

15. 根据权利要求 8 的装置，其中的鉴别信息除了包含有数字签名之外，还至少包括日期信息、位置信息、时间信息、装置的独特信息和签名人的专有信息中的一种。

16. 一种将鉴别信息嵌入数字信息的信息处理装置的控制方法，包括：

依据将要在其中嵌入鉴别信息的数字信息产生鉴别信息的步骤；和

将所产生的鉴别信息嵌入数字信息并使数字信息可恢复的数字水印形成步骤。

17. 一种用于鉴别数字信息的信息处理装置的控制方法，其中鉴别信息作为数字水印嵌入到数字信息中，该方法包括：

从数字信息提取出作为数字水印嵌入的鉴别信息作为第一鉴别信息的步骤；

数字水印消除步骤，用于消除从数字信息提取的作为数字水印的鉴别信息，并恢复推测的原始数字信息；

在数字水印消除步骤中，在通过消除数字水印而恢复推测的原始数字信息的基础之上形成第二鉴别信息的形成步骤；和

将第一鉴别信息和第二鉴别信息进行比较的比较步骤。

18. 由计算机装入并执行以使计算机成为将鉴别信息嵌入数字信息的信息

处理装置的计算机程序，包括：

在鉴别信息将要嵌入其中的数字信息的基础上产生鉴别信息的步骤的程序代码；和

将产生的鉴别信息嵌入可恢复的数字信息的数字水印形成步骤的程序代码.

19. 一种存储介质，存储了权利要求 18 中的计算机程序.

20. 由计算机装入并执行以使计算机成为将鉴别信息嵌入数字信息的信息处理装置的计算机程序，包括：

从数字信息提取出作为数字水印嵌入的鉴别信息作为第一鉴别信息的步骤的程序代码；

消除从数字信息提取的作为数字水印的鉴别信息，并恢复推测的原始数字信息的数字水印消除步骤的程序代码；

在数字水印消除步骤中，在通过消除数字水印而恢复推测的原始数字信息的基础之上形成第二鉴别信息的形成步骤的程序代码；和

将第一鉴别信息和第二鉴别信息进行比较的比较步骤的程序代码.

21. 一种存储介质，存储了权利要求 20 中的计算机程序.

22. 一种用于将附加信息嵌入到组成数字数据的元素的信息嵌入装置，该数字数据是通过从所述元素加上/减去一个值而得到的，该装置包括：

检测装置，用于检测这样的元素：在加运算/减运算之后，其值超越了能够认定的元素范围；

通过结合附加信息和由所述检测装置检测的信息而产生有效的嵌入信息的产生装置；和

嵌入装置，用于排除这样的元素：在嵌入到数字数据时，经过嵌入处理的加运算/减运算之后，其值超越了认定的元素范围，并将由所述产生装置产生的有效的嵌入信息作为数字水印嵌入到落在认定的元素范围之内的元素.

23. 根据权利要求 22 的装置，其中的数字数据为图像数据，并且

所述检测装置用于检测这样的像素位置：该像素在加运算/减运算之后其值超越了设定的像素值范围.

24. 根据权利要求 22 的装置，进一步包括对附加信息和被所述检测装置检测的信息中的至少一种进行压缩编码的编码装置，其中所述产生装置在所述编

码装置编码产生的结果的基础上产生有效的嵌入信息.

25. 根据权利要求 22 的装置，进一步包括对附加信息和被所述检测装置检测的信息中的至少一种进行加密的加密装置，其中所述产生装置在所述加密装置加密产生的结果的基础上产生有效的嵌入信息.

26. 根据权利要求 22 的装置，进一步包括将附加信息和被所述检测装置检测的信息中的至少一种转换为纠错码的编码装置，其中所述产生装置在所述编码装置转换结果的基础上产生有效的嵌入信息.

27. 根据权利要求 22 的装置，进一步包括用于校正数字数据以减少数字数据中元素数量的校正装置，该元素在加运算/减运算之后具有超越设定的元素范围的值，其中所述产生装置通过嵌入表示所述校正装置的校正指令的信息而产生有效的嵌入信息.

28. 一种信息恢复装置，用于接收由权利要求 22 中的信息嵌入装置将信息嵌入其中的数字数据，并恢复原始数字数据，该恢复装置包括:

数字水印提取装置，用于提取嵌入到输入的数字数据中的信息; 和

数字水印消除装置，用于依据表示未进行嵌入处理的元素的信息，从执行过嵌入处理的元素中消除嵌入的信息，并恢复原始数字数据.

29. 根据权利要求 28 的装置，进一步包括对由所述数字水印提取装置提取的附加信息和表示未进行嵌入处理的元素的信息中的至少一种进行解压编码的译码装置，其中所述数字水印消除装置在由所述译码装置译码得到的结果的基础上消除数字水印.

30. 根据权利要求 28 的装置，进一步包括对由所述数字水印提取装置提取的附加信息和表示未进行嵌入处理的元素的信息中的至少一种进行解密译码的译码装置，其中所述数字水印消除装置在由所述译码装置译码得到的结果的基础上消除数字水印.

31. 根据权利要求 28 的装置，进一步包括对由所述数字水印提取装置提取的附加信息和表示未进行嵌入处理的元素的信息中的至少一种的纠错码进行译码的译码装置，其中所述数字水印消除装置在由所述译码装置译码得到的结果的基础上消除数字水印.

32. 一种控制信息嵌入装置的方法，其中的信息嵌入装置用于将附加信息嵌入到组成数字数据的元素中，而数字数据是通过在所述元素加上/减去一个值

得到的，该方法包括：

检测步骤，检测在加运算/减运算之后，其值超越了设定的元素范围的元素；

通过将附加信息和在检测步骤中被检测的信息相组合而产生有效的嵌入信息的产生步骤；和

嵌入步骤，用于将加/减运算后超过了认定的元素范围的那些元素，排除在有关嵌入到数字数据内的嵌入处理之外，并且将在产生步骤中产生的有效的嵌入信息作为数字水印嵌入到落在设定的元素范围之内的元素。

33. 一种控制信息恢复装置的方法，该装置接收由权利要求 22 中的信息嵌入装置将信息嵌入到其中的数字信息，并恢复原始图像，该方法包括：

数字水印提取步骤，用于提取嵌入到输入的数字数据的信息；和

数字水印消除步骤，用于依据指出未进行嵌入处理的元素的信息，从进行了嵌入处理的元素中消除嵌入的信息，并恢复原始数字数据。

34. 一种计算机程序，它是由计算机装入并执行以使计算机成为用于将附加信息嵌入到组成数字数据的元素的信息嵌入装置，该数字数据是通过从元素加上/减去一个值而得到的，该计算机程序包括：

检测步骤的程序代码，用于检测在加运算/减运算之后其值超越了设定的元素范围的元素；

产生步骤的程序代码，通过将附加信息和在检测步骤中被检测的信息组合而产生有效的嵌入信息；和

嵌入步骤的程序代码，将在经过加运算/减运算之后，具有超越了认定的元素范围的值的元素排除在用于嵌入数字数据的嵌入处理之外，并将在产生步骤中产生的有效的嵌入信息作为数字水印嵌入到落到认定的元素范围的元素。

35. 一种计算机程序，它是由计算机装入并执行已使计算机成为这样一种信息恢复装置：接收由权利要求 22 中的信息嵌入装置将信息嵌入其中的数字数据并恢复原始数字数据，该计算机程序包括：

数字水印提取步骤的程序代码，用于提取嵌入到输入的数字数据的信息；和

数字水印消除步骤的程序代码，用于依据指出了未进行嵌入处理的元素的信息，从进行了嵌入处理的元素中消除嵌入的信息，并恢复原始数字数据。

36. 一种存储介质，存储了权利要求 34 中的计算机程序。

37. 一种存储介质，存储了权利要求 35 中的计算机程序。

说　　明　　书

信息处理装置及其控制方法、计算机程序和存储介质

技术领域

本发明涉及一种用于标识和鉴别数字信息的信息处理方法和装置及存储介质。

背景技术

近年来，计算机和网络飞速发展，多种数字信息例如文本数据、图像数据、音频数据等被利用。这些数据信息不会因为例如老化而损坏，并且能被永久地、良好地保存。而且数字信息能被容易的编辑和处理。这种做法对于编辑和处理数字信息的用户来说会更有利。

然而，对于在意外事件处理中使用证据照片的保险公司或是记录建筑场所的进展情况的建筑公司，数字数据比模拟数据的可靠性低，而且数字数据作为证据的证明力比较弱。

因此，检查任何篡改和/或伪造数字数据的视频输入装置和系统被提了出来。

例如，众所周知的一种使用数字签名的系统是用于检测任何篡改和/或伪造的系统。以下将简要介绍数字签名。

通过使用数字签名，发送器可以同时发送数据以及与该数据相应的特征数据，并且接收器通过检验特征数据而检查数据的可靠性。如下所述，利用散列函数和公共密码术而产生的数字签名检验数据的可靠性。

令 Ks 为一个密钥，Kp 为一公共密钥。那么，发送器通过利用散列函数来压缩纯文本数据 M 以执行一种算术运算，该算术运算用于计算出给定长度（例如 128 字节）的输出 h。发送器在经过这样的算术运算来产生数字签名数据 s：用密钥 Ks 变换 h，也就是，D(Ks, h)=s。之后，发送器发送数字签名数据 s 以及纯文本数据 M。

另一方面，接收器产生这样一种算术运算：用公共密钥 Kp 对接收到的数字签名数据 s 进行变换，即，E(Kp, s)=E(Kp, D(Ks, h″))=h″，同时产生这样一种

算术运算:通过使用与发送器相同的散列函数来压缩接收到的纯文本数据M以计算h′．如果h′和h″相匹配，接收器确定接收到的数据M′是可靠的．

如果纯文本数据M在发送器和接收器之间被篡改了，E(Kp, s)=E(Kp, D(Ks, h″))=hh″与通过使用与发送器同样的散列函数压缩接收到的纯文本数据M′而得到的h′不相匹配，则检测出数据被篡改．

如果对数字签名数据s的篡改和对纯文本数据M的篡改相一致，那么将无法检查到这种篡改．然而在这种情况下，纯文本数据M必须从h计算得出，但由于散列函数的单向性而不能产生这样的操作．如上所述，通过使用利用了公共密码术和散列函数的数字签名可以正确的鉴别数据．

下面将解释散列函数，散列函数用来以高速产生数字签名等．散列函数具有这样一种功能，它可以处理任意长度的纯文本数据M，并输出一确定长度的输出h．注意输出量h称为纯文本数据M的散列值（或者信息摘要，数字指纹）．散列函数需要有单向性和抗冲突性．单向性意味着如果h是确定的，在计算上就不可能得出满足h=H（M）的文本数据M．抗冲突性意味着如果文本数据M是确定的，在计算上就不可能得出满足H（M）=H（M′）的纯文本数据M′（M≠M′），也不可能计算出满足H（M）=H（M′）和M≠M′的纯文本数据M和M′．

作为散列函数，MD-2, MD-4, MD-5, SHA-1, RIPEMD-128, RIPEMD-160等等是公知的，并且这些算法是普遍的．

下面将介绍公共密码术．在公共密码术中，加密和解密密钥是不同的，加密密钥是公知的，而解密密钥是保密的．公共密码术具有如下特征，

(a) 既然加密和解密密钥是不同的而且加密密钥是公知的，那么不需要加密传送加密密钥，且很容易进行密钥传送；

(b) 既然每一个用户的加密密钥是公开的，用户只需将他或她的解密密钥保密；

(c) 可以实现接收器使用的一个鉴别函数来鉴别信息发送者是否是非法的，且信息是否被篡改；

例如，如果使用公共加密密钥Kp对纯文本数据M进行加密由E(Kp, M)表示，使用私人解密密钥Ks进行解密由D(Ks, M)表示，则公共密码术的算法满足下列两个条件:

（1）如果Kp已知，容易得到E(Kp, M)，如果Ks已知，容易得到D(Ks, M)．

（2）如果 Ks 未知，即使 Kp, E, C=E(Kp, M) 能够确定，在算法上也不能确定 M.

如果在满足上述条件（1）和（2）的同时，满足下面条件（3），则保密通信能够实现.

（3）可以将 E(Kp, M) 定义为用于所有文本数据 M 且 D(Ks, E(Kp, M))=M. 那就是说，既然 Kp 为公众所知，任何人都能得到 E(Kp, M)，但是只有知道私人密钥 Ks 的人才能通过计算 D(Ks, E(Kp, M)) 而得出 M. 如果在满足上述条件（1）和（2）的同时，满足下面条件（4），则能够实现鉴别通信.

（4）可以将 D(Ks, M) 定义为用于所有文本数据 M 且 E(Kp, D(Ks, M))=M. 那就是说，只有知道私人密钥 s 的人能够得到 D(Ks, M)，如果第三者将他或她伪装成了解密钥 Ks 的人，通过使用一个错误的密钥 Ks′ 计算 D(Ks′, M)，则由于 E(Kp, D(Ks′, M)) ≠M，所以接收器能够确定接收到的信息是非法的. 甚至当 D(Ks, M) 被篡改时，也会由于 E(Kp, D(Ks′, M)) ≠M，使接收器能够确定接收到的信息是非法的.

作为能够实现保密通信和鉴别通信的典型实施例，RSA 密码学，R 密码学，W 密码学等都是熟知的.

现代广泛使用的 RSA 密码学的加密和解密提供如下:

加密: 加密密钥（e, n）加密变换 $C=M^e \pmod n$

解密: 解密密钥（d, n）解密变换 $M=C^d \pmod n$

$n=p \cdot q$（这里 p 和 q 是两个完全不同的素数）

如上所述，由于 RSA 密码学在加密和解密中都要进行幂和余数的数学运算，所以与公共密码术例如 DES 等进行比较，需要巨大的数学运算量，也就不容易达到高速处理.

如上所述，为了发现在前的数据是否被篡改和/或伪造，除了数字数据之外还需要一数字签名. 一般的，数字签名被附加到数字数据的首部而发送. 然而，添加的数字签名很容易随着数字数据的格式变换而被消除. 如果数字签名被消除了，数字数据将不能被鉴别.

日本专利公开号 10-164549 所披露的方法能解决上述问题. 在日本专利 10-164549 中，数字信息被分成两个字段，数字签名产生于分割的第一字段，并且所述数字签名被嵌入分割的第二字段作为数字水印，从而产生签名的数字信

息。另一方面，鉴别装置将标记信息分割为第一、第二字段，从第一字段产生一第一数字签名，并且从第二字段提取出作为数字签名而被嵌入的一个第二标记。如果第一、第二数字签名相匹配，可以认定数字信息没有被篡改和伪造。

如上所述，为了鉴别数字数据，重要的一点是不能抛开数字信息而单独设定鉴别信息。在日本专利 10-164549 公开的方法中，由于为了鉴别原始图像签名信息是作为数字水印而被嵌入的，而且数字水印不能消除，所以不能获得原始图像。一些应用和用户可能将嵌入数字水印本身作为“篡改”。

发明内容

本发明是在考虑了前面提到的问题而提出的，本发明的目的是提供一种信息处理装置和控制方法、计算机程序和存储介质，能够在不脱离数字信息而设置鉴别信息的同时确定数字信息是否被篡改，并且只要数字信息不被篡改，就可恢复出原始的数字信息。

为了实现上述目的，例如，按照本发明，能够附加鉴别信息的信息处理装置包括下列结构。

也就是在数字信息处理装置中嵌入鉴别信息的信息处理装置包括:

在将要嵌入鉴别信息的数字信息的基础上产生鉴别信息的装置；和

将所产生的鉴别信息嵌入到可恢复的数字信息的数字标记装置。

另外，能够鉴别信息的信息处理装置包括如下结构。

即，能够鉴别其中嵌入有作为数字水印的鉴别信息的数字信息的信息处理装置包括:

从数字信息中提取出所嵌入的作为数字水印的鉴别信息作为第一鉴别信息的提取装置;

数字水印消除装置用于消除从数字信息提取的作为数字水印的鉴别信息并暂时恢复原始数字信息;

依据由数字水印装置消除数字水印、从而暂时恢复出的原始数字信息产生第二鉴别信息的发生装置；和

第一鉴别信息和第二鉴别信息比较单元。

通过参考附图所作的以下说明将使本发明的其它特征和有点更加明显，在所有附图中相同的参考标记表示相同或相似的部件。

附图说明

图 1 为应用于本发明实施例中的计算机方框图;

图 2 为本发明实施例的签名装置的方框图;

图 3 为本发明实施例中鉴别装置的方框图;

图 4 为图 2 所示数字水印装置的详细方框图;

图 5 为拼凑方法的原理解释图;

图 6 表示关于提取数字水印的可靠性间隔 d 的频率分布状态图;

图 7 为本发明实施例中数字水印单元的方框图;

图 8 为应用于本发明另一个实施例中的信息处理装置的方框图;

图 9 为本发明另一个实施例中的数字水印形成装置的方框图;

图 10 为本发明另一个实施例中的图像恢复装置的方框图;

图 11 示出了本发明另一实施例中的代码序列 w 的例子;

图 12 为本发明又一实施例中的数字水印形成装置的方框图;

图 13 为本发明又一实施例中的图像恢复装置的方框图;

图 14 示出了嵌入数字水印的过程的要点;

图 15 示出了恢复原始数据的过程的要点;

图 16 示出了嵌入数字水印时发生溢出的例子;

图 17 示出了溢出发生时原始数据不能恢复的例子;

图 18 为在本发明的另一个实施例中数字水印形成顺序的流程图;

图 19 为本发明另一个实施例中原始数据恢复顺序的流程图;

图 20 示出了本发明又一实施例中的代码序列 w 的例子;

图 21 示出了本发明又一实施例中用于解释纠错过程的像素分布状态的例子;

具体实施例

下面将结合相关的附图来描述本发明的最佳实施例.

下面将说明用于把鉴别信息嵌入信息的签名装置和用于鉴别所述信息的鉴别装置.

〈签名装置〉

下面将结合图 2 说明本实施例的签名装置.

参照图 2, 代号 201 代表图像输入单元; 202 代表散列值计算单元; 203 代表加密单元; 204 代表数字水印单元; 205 代表图像输出单元.

图像信号以光栅扫描顺序输入到图像输入单元201. 任何图像扫描仪、存储图像的存储介质、借助于通信接收来自于远程碟片的图像的通信装置等都可作为图像输入单元 201 的输入源. 下面介绍表示单色多值图像的图像信号. 如果图像信号表示含有许多色彩分量的彩色图像等的图像, 可将 R、G、B 色彩分量中的每一个或者亮度和色度分量中的一个当作单色分量来处理.

输入图像信号 I 被输入到散列值计算单元 202 和数字水印形成单元 204.

散列值计算单元 202 计算并输出一输入图像信号 I 的散列值 H. 使用散列函数来计算散列值 H. 本发明并未限定为特殊散列函数, 并且使用了例如 MD-2、MD-4、MD-5、SHA-1、PIPEMD-128、RIPEMD-160 等类似的、对公众也是熟知的不同算法. 算出的散列值 H 被输入到加密单元 203.

加密单元 203 利用私人密钥 S 给输入的散列值 H 加密并输出加密的散列值. 并未将本发明限制为用来加密的任何特殊的加密算法, 可以使用 RSA 密码术等作为公共密码术. 经过加密的散列值 Es(H) 输入到数字水印形成单元 204.

数字水印形成单元204将加密的散列值Es(H)作为可逆的数字水印嵌入到输入的图像信号 I, 并且输出该图像信号 (可逆的数字水印将在后面介绍). 将嵌有数字水印的图像信号 wI 输出到图像输出单元 205. 输出的对象没有特殊限制并且该图像信号可以输出到存储介质、通信线等上面.

〈鉴别装置〉

下面将通过图 3 介绍本实施例的鉴别装置.

参见图 3, 标号 301 表示图像输入单元; 302 表示数字水印提取单元; 303 表示解密单元; 304 表示散列值运算单元; 305 表示比较单元.

一图像输入信号 wI′ 以光栅扫描的顺序被输入到图像输入单元 301. 该输入图像 wI′ 又被输出到数字水印提取单元 302. 注意 wI′ 最好能与图 2 所示的特征单元的输出 wI 相等, 但是由于该输入图像信号可能被篡改或伪造, 所以它用 wI′ 表示.

数字水印提取单元 302 从输入的图像信号 wI′ 提取被嵌入的数字水印 E′s(H), 并消除可逆的数字水印. 然后输出被提取的数字水印 E′ s(H) 和消除了数字水印的图像信号 I′ .

如果 wI′ 等于 wI, 将提取 Es(H) 作为数字水印 (即 Es(H)= E′ s(H)). 此外, 在这种情况下, 可逆的数字水印将被完全消除, 并输出图像数据 I(即 I=

I′）．另外，如果wI′与wI不同，则不同于Es(H)的数据将被作为数字水印输出（即Es(H)≠E′s(H)）．此外，在这种情况下，并没有完全消除可逆的数字水印（即I≠I′）．

而且，如果数字水印被嵌入到输入的图像，数字水印提取单元302还有检测的功能．利用这项功能，如果其中没有作为数字信号而嵌入的数字签名的图像数据输出为wI′，则数字水印提取单元输出“无信息”，并且在稍后不执行鉴别处理．在这种情况下，将利用例如显示器输出一条信息“图像数据不能被鉴别”．

提取的数字水印E′s(H)被输出到解密单元303，消除了数字水印的图像数据I′被输出到散列值运算单元304．

解密单元303对输入的数据E′s(H)解密并将其输出．关于解密，将使用与在签名装置中使用的私人密钥s相对应的公共密钥p．被解密的数据H被输入到比较单元305．

散列值运算单元304将对输入的图像数据I′的散列值H′进行计算并将其输出．作为用来计算散列值的散列函数，该散列函数与在签名装置中使用的散列函数等同．计算得出的散列值H′将被输出到比较单元305．

比较单元305对输入的散列值H和H′进行比较以检验wI′是否被篡改或伪造了．如果H和H′彼此相等，则wI=wI′，也就是能够确定输入的数据没有被篡改或伪造．如果H和H′彼此不等，则wI≠wI′，也就是说能够确定输入的数据被篡改或伪造了．在这种情况下，将在显示设备上显示表明这一点的信息．

〈数字水印形成单元〉

下面将介绍本实施例的数字水印形成单元204的细节．简要的介绍一个过程，数字水印装置嵌入信息以便在嵌入数字水印之前完全恢复图像数据．

图4示出了数字水印形成单元204的内部结构．下面将参照图4介绍处理流程．

图像数据I被输入到数字水印形成单元204，并且一嵌入位置确定单元401确定将被嵌入到图像数据I的数字水印的嵌入位置．该图像数据I被输入到附加信息嵌入单元402，并且依照附加的信息Es(H)在由嵌入位置确定单元401确定的位置嵌入数字水印．

为了实现上述目的，嵌入位置确定单元 401 将输入的图像数据 I 和指示图像位置的数据(指定了每一个区域的坐标和大小)输出到附加信息嵌入单元 402；其中所述的图像位置是将要嵌入附加信息 Es(H) 的一个位置。

除了图像信息 I 之外，附加信息嵌入单元 402 还接收附加信息 Es(H)（若干位的信息）。通过使用数字水印技术，附加的信息 Es(H) 将在所确定的图像数据 I 的嵌入位置被嵌入。随后将介绍利用数字水印技术嵌入附加信息 Es(H)。附加信息嵌入单元 402 输出嵌入了附加信息 Es(H) 并且经数字水印处理的数据 wI。

在本实施例中，为了简化的目的，输入到数字水印装置的数据为每像素(256 个灰度级）具有 8 比特灰度精度的灰度图像数据。然而，输入图像数据可能为彩色图像数据。当输入彩色图像时，利用彩色图像的一个信道的像素值或彩色图像的亮度值，则可以执行一个相似的嵌入处理。

当输入音频信号时，图像的 2 维位置信息将被作为时间的 1 维信息，可以使用相同的执行方案。当输入移动图像数据时，由于它可被看作是沿时间轴方向的多个二维图像，所以能用相同的方案处理每一个二维图像，基本应用了本发明。因此，本发明的范围也包括数字水印嵌入到彩色图像、音频和活动图像的情况。

下面将介绍本实施例中数字水印的嵌入和分离（提取）的基本原理。

〈拼凑方法〉

本实施例使用称为拼凑方法的原理来嵌入附加的信息 Inf(与上述实施例中的 Es(H) 一致)。拼凑方法在 1997 年 2 月 24 日出版的 Nikkei Elctronics，由 Walter Bender、Daniel Gruhl、Norishige Morimoto 和 Anthony Lu 等提出的 “Data Hiding Technique that Supports Digital Watermarking(Vol. 1)” 有所披露。首先将介绍拼凑方法的原理。

在拼凑方法中，通过在统计上偏离图像，可以嵌入附加信息 Es(H)。

下面将通过图 5 来介绍拼凑原理。图 5 中，A 和 B 是从一原始图像中选出的两个子集。假定子集 A 是由许多子集 a_i501 表示的子集组成的，而子集 B 是由许多子集 bi502 表示的子集组成的。

如果这两个子集不互相重叠，那么通过本实施例的拼凑方法可以嵌入附加信息 Inf。

假定子集 A 和 B 中的每一个都包含 N 个元素（$A=\{a_1, a_2, \cdots, a_N\}$，

$B=\{b_1, b_2, \cdots, b_N\}$)。子集 A 和 B 中的元素 a_i 和 b_i 表示具有像素值的像素或一组这样的像素。

下一个指数 d 定义为 $d=1/N \cdot \Sigma (a_i-b_i)$，此处 Σ 为 i=1 至 N 的和。

这就表示出了两组像素值之间不同的期望值。

当从一般自然的图像中适当选择子集 A 和 B 并且定义指数 d，如果 N 的值足够大，我们将得到:

$d \approx 0$

在下文中 d 将被作为可靠性间隔。

另一方面，作为组成附加信息 Es(H) 的各个位嵌入操作，例如，当嵌入位信息“1”时，将产生这样的操作:

$a'_i = a_i + c$

$b'_i = b_i - c$

这样的操作将在子集 A 的所有元素的像素值加上“c”，而对子集 B 的所有元素的像素值都减去“c”。在本实施例的下文中“c”将被作为“嵌入深度”。

象上面的情况，当从一图像中选择了嵌入附加信息 Es(H) 的子集 A 和 B，指数 d 为:

$$d=1/N \cdot \Sigma (a_i-b_i)$$
$$=1/N \cdot \Sigma \{(a_i+c)-(b_i-c)\}$$
$$=1/N \cdot \Sigma \{(a_i-b_i)+2c)\}$$
$$\approx 2c$$

(Σ 为 i=1 至 N 的和)

也就是说，d 呈现为这样一个值，它与 0 相差一给定间隔。

为了嵌入其它的位信息（位信息“0”），将执行以下操作:

$a'_i = a_i - c$

$b'_i = b_i + c$

那么可靠性间隔 d 为:

$$d=1/N \cdot \Sigma (a_i-b_i)$$
$$=1/N \cdot \Sigma \{(a_i-c)-(b_i+c)\}$$
$$=1/N \cdot \Sigma \{(a_i-b_i)-2c)\}$$
$$\approx -2c$$

也就是间隔 d 假定为这样一个值，它在负方向上与 0 相差一个给定的距离.

当给定了某一图像，通过计算图像的可靠性距离 d，就能够确定图像中是否嵌入了附加信息.

即：如果可靠性距离 d≈0，则没有嵌入附加信息 Es(H)；如果可靠性距离 d 为一预先确定的正值或为比 0 大得多的值，则嵌入位信息“1”；如果可靠性距离 d 为一预先确定的负值或为比 0 小得多的值，则嵌入位信息“0”.

本实施例中，通过利用先前提到的拼凑方法原理，可以在单一的图像中嵌入大量位信息片段.

本实施例中，在单一图像的不同区域，不但可以采用子集 A 和 B 的组合，而且可以采用许多子集 A′ 和 B′ 、A″ 和 B″ 、…的组合来嵌入包含有许多位的附加信息 Es(H)。注意子集 A 和 B、A′ 和 B′ 、A″ 和 B″ 、…的分布不能重叠.

下面将检验从其中嵌入了大量位信息的数据中提取位信息的方法.

图 6 中标号 601 表示从没有嵌入数字水印的数据中计算得出的可靠性距离 d 的分布状态. 分布曲线 601 示出了最有可能出现的可靠性距离 d 的值，因为对应该可靠性距离 d 的出现频率的分布较大.

分布曲线 602 和 603 分别为由嵌入了位信息“1”和位信息“0”的数据计算得到的可靠性分布距离 d.

同样地，每个分布曲线 602 和 603 分别示出了最有可能出现的可靠性距离 d 的值，因为对应该可靠性距离 d 的出现频率的分布较大. 注意一个位信息对应一个可靠性距离 d.

图 6 中的分布曲线 601、602、603 都为正态分布状态. 下面将利用中心极限定理来介绍该正态分布曲线的组成原因.

〈中心极限定理〉

该定理揭示了：当从具有均值 m_c 和标准误差 δ_c 的全体域（不需要为正态分布）中随机抽取大小为 n_c 的样本时，具有样本均值 s_c 的分布近似于具有增大的 n_c 的正态分布 $N(m_c, s_c/\sqrt{n_c})^2$.

一般地，全体域的标准误差 δ_c 是未知的，然而，如果样本数 n_c 足够大，且全体域中的数 N_c 足以比样本数 n_c 更大，那么在常规的做法中，可以使用样本的标准误差 s_c 来代替 δ_c.

本实施例中，每个子集 A 和 B 都包括 N 个元素（$A=\{a_1, a_2, \cdots, a_N\}$，$B=\{b_1, b_2, \cdots, b_N\}$），且这些集合为具有子集 A 和 B 元素的像素值，如

图 5 所示. 如果设定 N 足够大且像素值 a_i 和 b_i 没有关联，则可靠性间隔 d($\Sigma(a_i-b_i)/N$)的期望值变为 0. 正如从中心极限定理能够得知：该可靠性间距 d 构成了一正态的分布.

因此当从可靠性间距 d 确定嵌入的位信息时，将在 0 到可靠性间距 2c 之间引入一个适当的门限值，并且当可靠性间距的绝对值比门限值大时，则确定信息已被嵌入，则在统计上完成了信息的可靠提取.

例如，令 δ 为正态分布 601 的标准误差. 那么，如果没有嵌入附加信息，则在图 6 阴影部分所示出的-1.96δ 到+1.96δ（95%的可靠性范围）的范围内，可靠性间距有 95%出现的可能性.

因此，在门限值范围以外出现可靠性间距 d 的概率随着门限值的增加而降低. 则能够提取高可靠性信息.

另外，如果设定一个大的嵌入深度“c”，则正态分布 602 和 603 将从分布状态 601 分离开，因而能设置一个大的临界值.

如果子集 A 和 B 中的元素数 N 是大的，则正态分布 601、602 和 603 的标准误差 δ 变小，并且如果嵌入深度 c 保持不变，则能确定更高的可靠性.

已经介绍了拼凑方法的基本思想.

本实施例中，数字水印形成单元 204 和数字水印提取单元 30 就是使用前述的拼凑方法.

下面将介绍常规的述字水印嵌入、提取和消除方法.

〈嵌入位置确定单元〉

由于拼凑方法嵌入包括许多位的附加信息，每个位信息都需要子集 A 和 B. 因此，为了嵌入多条位信息，必须确定 A 和 B、A′ 和 B′、A″ 和 B″、…的位置.

图 4 的嵌入位置确定单元 401 确定需要嵌入若干条位信息的嵌入位置. 作为一个简单的嵌入位置确定方法，可能使用利用随机数来确定位置的方法. 许多比特以良好的稳定性嵌入整个图像，以便相应的子集元素几乎是均匀分布的，而且子集之间不互相重叠.

例如，简要介绍使用与图像具有同样大小的白噪声掩码的方法.

白噪声掩码是由二维分布的掩码像素组成的，每个掩码都有一个在 0 至 255 范围内的系数. 在 0 至 255 之间的白噪声掩码的每个系数都被赋予了差不多相

同数目的掩码像素.

例如，当原始图像具有2000 ×2000像素（=4000000个像素）时，由于一个白噪声掩码配置了与原始图像像素数相同的掩码像素数，则有15625（=4000000/256）个掩码像素具有“0”值. 这样的掩码像素是随机分布的，以形成白噪声掩码.

因此，一旦嵌入1比特附加信息，则当将具有奇数灰度级的掩码像素指定给子集A，而将具有偶数灰度级的掩码像素指定给子集B时，则子集A和B具有相同的像素数且互相不重叠，而附加信息能以良好的稳定性嵌入整个图像.

当嵌入许多（M）条位信息时，像素数被均匀的分配给每个位信息（1至M）（例如，将设定的白噪声掩码的范围除以2M，余数均匀的分配给子集A或B），则嵌入多条位信息.

如果每个像素都用8比特表示，则由于灰度级数为256，因而能嵌入的最大的比特数M为128. 该最大值仅满足一个散列值（64或128比特），但如果加入另外的信息（如版权保护信息），该值将不充分. 然而，当一幅图像被分割为四部分，且为相关的分割块配置白噪声掩码，则能嵌入128 ×4=512比特. 如果分割块数大于4，嵌入的比特数也会增加. 然而，如果分割块数增加，则由于正态分布很难形成，所以嵌入信息的提取可能会经常失败. 因此，确定分割块数应与原始图像的大小相应.

因此嵌入位置确定装置仅需产生事先准备的掩码模式. 注意在嵌入中使用的、相同的掩码是在提取和分离数字水印的一侧准备并使用的.

〈附加信息嵌入单元〉

附加信息嵌入单元402接收图像数据I、附加信息$E_S(H)$，以及如上所述的由嵌入位置确定单元401确定且与相应的比特一致的嵌入位置.

按照组成输入的附加信息$E_S(H)$的位信息，计算与每个二进制数相对应的子集A和B的像素的像素值.

如在拼凑方法部分中介绍的，如果位信息为“1”. 则从子集A的像素的像素值加上“C”，而从子集B的像素的像素值减去“C”. 如果位信息为0，则从子集A的像素的像素值减去“C”，而把子集B的像素的像素值加上“C”. 通过前述的处理，附加信息嵌入单元402嵌入附加信息$E_S(H)$.

通过前述方法可以嵌入附加信息. 然而，如果执行上面的方法，同时满足

c>a_i或a_i〉255-c 和 c〉b_i或b_i〉255-c 的嵌入的像素的像素值a_i'和b_i'变为a_i'（b_i'）〈0 或a_i'（b_i'）〉255. 因此数字水印消除单元（后面将介绍）在这些像素位置不能恢复原始图像的像素（即a_i和b_i）.

本实施例用于实现满足这样的条件的像素的嵌入处理: c≤a_i≤255-c 和 c≤b_i≤255-c，而对落在该范围之外的像素值不执行任何嵌入. 所以，在上面的叙述中，当嵌入 M 比特时，“白噪声掩码呈现的范围被划分成 2M 份”，但必须提前排除那些范围. 注意不进行嵌入处理的像素的位置信息必须作为溢出位置信息输出，并输入到数字水印提取单元和数字水印消除单元（后面将介绍）.

〈数字水印提取装置〉

下面将介绍本实施例中的数字水印提取装置 302. 数字水印提取装置 302 具有如图 7 所示的结构.

如图 7 所示，数字水印提取装置 302 包括嵌入位置确定单元 701、附加信息提取单元 702、统计测试单元 703、比较单元 704 和附加信息消除单元 705.

数字水印提取装置接收数字水印嵌入数据 wI′. 嵌入位置确定单元 701 产生在该位置处嵌入数字水印（与在数字水印形成装置 204 中使用的白噪声掩码相同的模式）的位置信息. 在输入的将要从其嵌入数字水印的位置信息的基础上，对于数字水印嵌入数据，附加信息提取单元 702 执行一预定的过程，则计算与嵌入到图像数据 wI′ 内的附加信息 E′$_s$(H)相对应的可靠性间距 d. 统计测试单元 703 统计测试与由附加信息提取单元 702 计算的附加信息 E′$_s$(H)相对应的数据的精度. 如果确定附加信息 E′$_s$(H)足够精确，则比较单元 704 提取附加信息 E_s(H). 如果附加信息不准确，则输出“无信息”. 如果嵌入了信息，附加信息消除单元 705 利用输入的图像数据 wI′、来自于嵌入位置确定单元 701 的嵌入位置信息和溢出位置信息来消除数字水印.

下面将详细介绍用于从嵌入有数字水印的图像数据 wI′ 来提取附加信息 E′$_s$(H)的数字水印提取单元的操作.

〈嵌入位置确定单元〉

嵌入位置确定单元 701 确定从其提取出附加信息 E′$_s$(H)的图像数据 wI′ 的区域. 嵌入位置确定单元 701 执行与嵌入位置确定单元 401 相同的操作. 由此单元 401 和 801 确定相同的嵌入位置. 确定的嵌入位置信息被输出到附加信息提取单元 702 和附加信息消除单元 705.

〈附加信息提取单元〉

附加信息提取单元 702 计算与每个比特相对应的可靠性间距 d，该比特来自于嵌入位置确定单元 701 确定的嵌入位置．在这种情况下，由于像素中没有嵌入附加信息，单元 702 不使用在计算可靠性距离 d 中由输入的溢出位置信息表示的像素．

〈统计测试单元〉

统计测试单元 703 统计的分析与从附加信息提取单元 702 输出的每个比特相对应的可靠性距离 d 的精度．如果嵌入了多条位信息，将获得多个可靠性间距 d．如果嵌入附加信息 $E'_s(H)$，则可靠性间距 d 出现在与图 6 内中心 0 相距 2c 的一个位置上．

这时，随着增大的嵌入深度 c，可靠性距离 d 出现在离图 6 中心 0 更远的位置上．因此，如果门限值限定在位置 c，而且获得比 c 大的可靠性间距 d，则确定嵌入的位信息为“1”；如果获得可靠性距离 d 比-c 小，则确定嵌入的位信息为“0”．

因此，，随着嵌入深度“c”的增加，一旦嵌入附加信息，正态分布 601、602 和 603 之间的间隔也随之增加，并确保提取信息的更高可靠性．同时，随着子集 A 和 B 的元素数 N 的增大，正态分布 601、602 和 603 的标准误差随之下降．因此，通过增加嵌入深度“c”以及子集 A 和 B 的元素的数目 N，即使在门限值为“c”时，也能得到高可靠性的提取信息．

注意当没有嵌入信息时，可靠性间距 d（更可能的）出现在从-c 到 c 的一个窄范围内而且通过利用该因素可以确定这样的情况．

尤其是，当与若干比特相应的给定数目的或更多数目的可靠性距离 d 出现在范围-c 到 c 之间时，本实施例的统计测试单元 703 确定没有嵌入信息，并显示一条消息来表示这样的结果．

〈比较单元〉

图 7 中的比较单元 704 被提供有与经过附加信息提取单元 702 和统计测试单元 703 输出的各条位信息相对应的可靠性间距 d 的值．

由于与输入到比较单元 704 的若干条位信息相对应的可靠性间距 d 是高度可靠的，那么仅仅依据与每个位信息相应的可靠性间距 d 的正负号来确定是“1”或“0”．

尤其是，如果给定的用于组成附加信息 $E'_s(H)$ 的位信息的可靠性间距 d 比“c”大，则确定出该位信息为“1”，如果可靠性间距 d 比“-c”小，则确定该位信息为“0”.

〈附加信息消除单元〉

下面介绍附加信息消除单元 705 执行的操作. 附加信息消除单元 705 接收附加信息 $E'_s(H)$ 的嵌入位置、图像数据 wI′ 和溢出位置信息，并输出其中消除了附加信息的图像数据 I′ .

在与数字水印形成单元中附加信息嵌入单元 402 嵌入的位置相同的位置上，在嵌入时通过改变嵌入深度“c”的符号将嵌入深度“c”加到与相应的比特相匹配的子集，以此来消除附加信息并恢复原始图像.

尤其在组成附加信息 $E'_s(H)$ 的预定的位信息的嵌入位置，如果位信息为“1”，则执行操作:

$$a'_i=a_i-c$$

$$b'_i=b_i+c$$

如果位信息为“0”，则执行操作:

$$a'_i=a_i+c$$

$$b'_i=b_i-c$$

则在嵌入前恢复像素值. 在这种情况下，利用了输入的溢出位置信息. 因此，由于在溢出位置上的像素中没有嵌入附加信息，该像素不用进行消除.

通过前面提到的运算，附加信息消除单元 705 从嵌入了数字水印的数据 wI′ 中消除了数字水印并输出其中的消除了数字水印的图像数据 I′ .

在前述的实施例中介绍了使用数字签名作为鉴别信息的方法. 然而，本发明不局限于该特殊的方法，包括例如，使用 MAC(消息鉴别码)作为鉴别信息的方法. 另外，除了数字签名和 MAC,还可能包括至少一个或更多的日期信息、位置信息、时间信息、装置的独特信息和签名人的专有信息.

此外，在上面的实施例中，使用的附加信息可以转换为纠错码. 通过这种方式可以进一步改善提取的附加信息 Inf 的可靠性.

注意在嵌入信息的一端和鉴别嵌入的信息的一端可以通过软件来实现装置的大部分组合元件，即图 2 和图 3 中所示的相关处理装置能由软件来实现.

在这种情况下，装置的结构可以是这样一种通用的装置: 普通个人电脑或

类似装置，例如，能使用图 1 所示的结构.

图 1 示出了应用于本实施例的图像处理装置的总体结构. 参照图 1，主机 101 为例如广泛使用的个人电脑.

在主机 101 内，通过总线 107 把下面将要介绍的相关部分连接起来以交换不同的数据.

参照图 1，标号 103 表示 CPU，它能控制相关内部单元的操作或执行内部存储的程序. 标号 104 表示一能存储引导程序和 BIOS 的 ROM. 标号 105 表示一暂时存储用于 CPU 执行操作时的程序或将要处理的图像数据的 RAM. 标号 106 表示一硬盘（HD），它能预先存储将要传送到 RAM 或类似单元的程序和图像数据，并能保存处理过的图像数据. 当主机作为签名装置使用时，硬盘 106 存储与图 2 相应的、在操作时被调入 RAM 105 的程序. 当主机作为鉴别装置使用时，硬盘 106 存储与图 3 相应的、在操作时被装入 RAM 105 的程序.

标号 108 表示一 CD 驱动装置：它能装入存储在作为一种外置的存储介质 CD(CD-R)上的数据，或者将数据写在 CD-R 上. 标号 109 表示一与 CD 驱动装置 108 类似的且能从 FD 装入数据或将数据写入 FD 的 FD 驱动装置. 标号 110 表示一与 CD 驱动装置 108 相似的且能从 DVD 装入数据或将数据写入 DVD 的 DVD 驱动装置. 注意当图像编辑程序或打印机驱动程序存储在 CD、FD、DVD 或类似物上时，这样的程序在需要时被装入 HD 106 并传送到 RAM 105. 这些存储介质用来存储原始图像，并在存储的图像中嵌入特征信息，或者鉴别存储在现有存储介质上的标识图像.

标号 113 表示一连接到键盘 111 和鼠标 112 以接收从其输入的指令的接口（I/F）. 标号 114 表示一包括有图像控制器和视频存储器（未示出）的显示控制器，用以产生与显示有关的控制，并通过把映射到视频存储器上的图像输出到显示设备 115 来显示图像. 标号 115 表示用于连接到互联网的通讯接口（例如，调制解调器、以太网转换器或类似装置）. 通过通信接口 115 能发送或接收附加有特征信息的信息.

注意用于输入图像数据的装置不局限于前面提到的装置，也可代之以扫描仪或类似物.

如上所述的，依据本实施例，数字信息和签名信息以不可分割的状态设置，而且签名信息经过类似的格式变换而被发送到鉴别装置.

[变换类型]

在上述实施例中，应用了拼凑方法。下面的叙述中将介绍本申请的其它例子。

如上所述，“数字水印”是公知的一种版权保护技术。数字水印是用于以一种看不见的形式在数字图像数据、音频数据、文本数据或类似的数据中嵌入版权所有者的名字或买主的 ID，并且跟踪利用非法拷贝进行的不预先通知所使用。由于数字可能遭受不同的破坏，则它必须具有抵抗破坏的强度。

另外提出了从图中提取嵌入的作为数字水印的信息并且从该图像完全恢复原始图像的技术。

一种嵌入方法简单的表示为：

$$I'_{j,i}=I_{j,i}+c_j \times a_i \times x_i \qquad (1)$$

其中 j 为表示附加信息 Inf 的区域和比特位置的正数，i 为表示像素位置的正数，$I'_{j,i}$ 为嵌入了数字水印的图像，如果 Inf_j=“1”，则 c_j 为常数+1，如果 Inf_j=“0”，则 c_j 为常数-1，a_i 为加权系数，而 x_i 为落在-1 到+1 之间的伪随机数序列。x_i 称为用来嵌入数字水印的载波信号。

在恢复操作时，首先提取嵌入的数字水印。利用提取的数字水印，通过下述等式恢复原始图像：

$$I''_{j,i}=I'_{j,i}-c_j \times a_i \times x_i \qquad (2)$$

其中 $I''_{j,i}$ 为被恢复的图像数据，$I'_{j,i}$ 为输入到图像恢复装置的图像数据，如果由数字水印提取单元提取的附加信息 Inf 中的位元为“1”，则 c_j 为常数+1，如果位元为“0”，则 c_j 为常数-1，而 a_i 和 x_i 与等式（1）中表示的相同。

下面将详细介绍等式（1）给出的数字水印的形成和等式（2）给出的原始图像恢复。

图 14 示出了由等式（1）给出的数字水印的形成的例子。各个矩阵表示图像的各个部分。图 14 示出了位信息为 1 即 c_j =+1 的情况。

在恢复端，首先提取数字水印。下面简要介绍该提取算法。检测在输入图像 I′ 的一个 4 ×4 的像素区域内的像素值和一个伪随机数序列 x_i（如上所述的，与在嵌入侧产生的随机数序列相同）之间的相关性。如果输入的图像 I′ 和伪随机数序列 x_i 之间的相关性高，则确定嵌入的位元为“1”。另外，如果输入的图像 I′ 和-x_j(通过改变相应的伪随机数序列的元素的符号而获得的结果)之间的

相关性高，则确定嵌入的位元为“0”．如果两个相关性都低，则确定没有嵌入数字水印信息．在图 14 中解释了 4 ×4 像素区．然而，如果一个位元仅仅嵌入到一个区域，则不能期望得到高精度．如图 14 所示，对许多区域（例如 n 像素区）采取这样的方法来改善整体的精度．如果嵌入了 m 个位元，则重复 m 次向 n 像素区中嵌入一个位元这样的过程．

在以这样的方式提取数字水印之后，执行消除该数字水印信息的过程．

图 15 示出了消除图 14 所示的例子中嵌入的数字水印的过程．在这种情况下，嵌入的位信息为“1”．如图 14 和 15 所示，一般情况下可完全消除嵌入的数字水印并恢复原始图像．

另外，图 16 也示出了由等式（1）给出的数字水印形成的例子．在图 16 所示的例子中，嵌入有数字水印的图像数据包括溢出的像素（那些在数字水印的形成之后具有像素值“262”和“261”的像素）．在这种情况下，采取了图 16 所示的舍入处理．数字水印可能从没有进行任何舍入处理的图像中被正确的提取，但是原始图像不能从进行了舍入处理的部分完美的恢复．

本质上，通过前面提到的方法，可从嵌入有数字水印的数字数据恢复在数字水印形成之前的数字数据，但是如果由于数字水印的形成而发生了溢出，则不可能完全的恢复在数字水印形成之前的数字数据，如上所述．注意溢出是这样一种现象：如果 $I_{i,j}$ 由 0 到 255 之间的整数（8 位）表示，在经过等式（1）的处理后，$I'_{i,j}$ 具有落在该范围之外的值．小于 0 的值通常被舍入为 0，大于 255 的值通常被舍入为 255．如果执行了这样的舍入处理，则不可能通过数字水印消除装置完全的消除数字水印．

由于这个原因，则很难在发生溢出的地方完全恢复原始图像部分．

因此本实施例能够实现原始数字数据的完美再现．

[数字水印的形成]

下面将介绍本实施例中的数字水印形成装置．本实施例中的数字水印形成装置嵌入附加信息以便能够完美的再现在数字水印形成之前的图像数据．

图 9 示出了数字水印形成装置的内部结构．下面将利用图 9 来解释数字水印形成装置的处理流程图．

图像 I 被输入到数字水印形成装置．为了简化，图像 I 为具有每像素 8 比特精度的灰度多值图像数据．然而，本发明不局限于这样的特定数据，而且可

能输入具有预定数目比特的灰度多值图像数据. 另外, 当输入一包括有许多元素的彩色图像时, 可以选择一个或许多元素作为输入的图像或图像组. 该输入的图像 I 被输入到溢出区域检测单元 2201 和数字水印形成单元 2203.

首先将介绍溢出区域检测单元 2201. 该溢出区域检测单元 2201 接收图像 I, 并且如果由下一个数字水印形成单元 2203 进行的数字水印形成处理后发生了溢出, 则检测用于组成输入的图像 I 的所有像素, 提取发生溢出的所有像素的位置. 同时输出这些像素的坐标信息.

在下面的叙述中, 发生溢出的像素 (0, 1, 或在某些情况下更多) 的位置信息将用溢出信息 R 来指代. 溢出信息 R 将被输出到编码单元 2202 和数字水印形成单元 2203. 后面将更详细的介绍溢出区域检测单元的操作.

下面将介绍编码单元 2202. 编码单元 2202 接收溢出信息 R 和附加信息 Inf, 并把该溢出信息 R 和附加信息 Inf 组合为一简单的代码序列, 并输出该组合的代码序列 w. 例如, w 具有图 11 所示的格式. 注意 w 用来将作为数字水印的代码序列由数字水印提取单元 2203 嵌入到图像 I. 由于这个原因, 为了实现有效的数字水印形成处理, 可以对 w 进行压缩编码. 另外, 如果附加信息 Inf 为私人信息, 可加密 w. 为了即使在嵌入了作为数字水印的附加信息 Inf 和将把该附加信息作为不同破坏的结果而变更为另一种信息之后, 也可以正确提取附加信息 Inf, 可把 w 转换为纠错码. 在任何情况下, 从嵌入处理开始, 都包含有由溢出信息 R 所指示的像素位置, 并且利用了在那些位置的原始图像的像素值.

下面将介绍数字水印形成单元 2203. 数字水印形成单元 2203 接收图像数据 I、溢出信息 R 和代码序列 w, 把代码序列 w 作为数字水印嵌入到图像 I, 并输出嵌入有数字水印的图像 I′. 注意由溢出信息 R 所指示的像素不进行数字水印的形成处理. 因此数字水印形成单元 2203 不会产生任何由于数字水印的形成而引起的溢出. 后面将更详细的介绍数字水印形成单元 2203 的操作.

如上所述的, 将作为数字水印的附加信息嵌入到图像 I, 则产生嵌入有数字水印的图像 I′.

[图像恢复装置]

下面将用图 10 来介绍本实施例的图像恢复装置. 图像恢复装置执行这样的过程, 用以把嵌入有数字水印的图像恢复为在数字水印形成之前的图像数据.

图像恢复装置通过前面提到的方法接收嵌入有数字水印的图像 I′. 该输入

的图像 I′ 被输入到数字水印提取单元 2301 和数字水印消除单元 2303.

首先解释数字水印提取单元 2301. 数字水印提取单元 2301 接收嵌入有数字水印的图像 I′，提取嵌入的代码序列 w，并输出该提取的代码序列 w. 数字水印提取单元 2301 使用输入的图像 I′ 的所有真实像素来提取数字水印. 也就是说，对所有像素连同那些由溢出信息 R(在由溢出信息 R 所述的位置没有嵌入数字水印)表示的并排除在数字水印嵌入目标之外的像素进行数字水印提取. 后面将更详细介绍数字水印提取单元 2301 的操作. 提取的代码序列 w 输出到译码单元 2302.

下面将介绍译码单元 2302. 译码单元 2302 接收由单元 2301 提取的代码序列 w，把它分为组成代码序列 w 的溢出信息 R 和附加信息 Inf，并输出该分割的溢出信息 R 和附加信息 Inf. 当编码单元 2202 对 w 进行压缩编码，译码单元 2302 执行解压译码的处理. 同时，当编码单元 2202 对 w 进行加密后，译码单元 2302 执行一个解压译码的处理以对加密数据解密. 另外，当编码单元 2202 把 w 转换为纠错码时，译码单元 2302 执行纠错译码处理以便纠正错误. 溢出信息 R 和附加信息 Inf 被输出到数字水印消除单元 2303.

下面将介绍数字水印消除单元 2303. 数字水印消除单元 2303 接收嵌入有数字水印、溢出信息 R 和附加信息 Inf 的图像 I′，利用附加信息 Inf 在执行数字水印之前从嵌有数字水印的图像 I′ 中恢复出原始图像，并输出该恢复的图像 I. 在该恢复处理中，排除了由溢出信息 R 指示的像素. 这是因为在通过前述的数字水印形成单元 2203 由溢出信息 R 指示的像素没有嵌入数字水印. 后面将更详细的介绍数字水印消除单元 2303 的操作.

如上所述的，从嵌入有数字水印的图像 I′ 恢复出在形成数字水印之前的图像 I.

[数字水印处理的细节]

下面将举例说明形成数字水印的细节.

下面将分析 n 比特信息 Inf 嵌入图像 I(即嵌入上述实施例的信息 w)的情况. 在这种情况下，图像 I 被分割为 n 个不重叠的区域 I_j(j=1, 2, …, n). 那么数字水印的形成过程给定为:

$$I'_{j,i}=I_{j,i}+c_j \times a_i \times x_i \quad (4)$$

其中 j 为表示附加信息 Inf 的区域和位元位置的正数，I 为表示像素位置的

正数，$I'_{j,i}$为嵌入有数字水印的图像，如果 Inf_j= "1"，则 c_j为常数+1，如果 Inf_j= "0"，则 c_j为常数-1，a_i为加权系数，而 x_i为落在范围-1 到+1 之间的一伪随机数序列．x_i称为用于实现嵌入数字水印的载波信号．

令 a_{max}为加权系数呈现的最大值（正值），而 x_{max}为 x_i所能达到的最大值（正值）．那么仅当满足条件：

$$a_{max} \times x_{max} \leqslant I \leqslant 255 - a_{max} \times x_{max} \quad (4)$$

时执行等式（3）给定的算术操作．

在这种情况下，由于 a_i和 x_i的相应元素值是同步出现的，并且在用于嵌入数字水印的装置和提取数字水印的装置中时已知的，等式（4）可进一步扩展为：

$$a_i \times x_i \leqslant I \leqslant 255 - a_i \times x_i \quad (4')$$

如果不满足等式（4）（或等式(4′)）的条件，则把像素位置记录为溢出信息 R．在普通的自然图像中，不满足等式（4）给定的条件的像素数（也就是排除嵌入的像素数）比整个图像的像素总数小的多．这表明溢出信息 R 有相对小的信息量．因此，当通过编码单元 2202 将溢出信息 R 作为代码序列 w 进行组合而后通过数字水印形成单元 2203 将代码序列 w 作为数字水印嵌入时，该信息大小也是忽略不记的．如上所述，由于在满足等式（4）（或等式(4′)）给定的条件下通过等式（1）嵌入数字水印，则能没有溢出地执行数字水印形成过程．

[图像恢复处理的细节]

下面将举例说明图像恢复处理的细节．

代码序列 w 作为数字水印而嵌入到输入的图像 I′．为了使用等式（3）来提取数字水印，从用于嵌入数字水印的载体信号 x 和输入到数字水印提取单元的图像 I′来计算 PFA，而且无论是否嵌入了数字水印，也无论位元为 "0" 还是 "1"，在计算结果的基础上确定是否嵌入了数字水印．

注意 PFA 表示实际上没有嵌入数字水印时，错误检查数字水印的概率．为了计算该概率，使用了称为统计测试的方法．统计测试对于本领域技术人员来说是公知技术．关于提取数字水印时使用统计测试的例子的更详细的说明，参考 1996 年 9 月出版的 I.C.I.I.P 会刊，215 至 218 页 I.Pitas 著的 "A method for signature casting on digital images"．利用统计测试，为每个位元进行计算以测试值 q_j．该测试值 q_j遵循零均值和误差=1 的标准正态分布，但当数字数据中嵌入有数字水印时，它遵循非零均值和误差=1 的正态分布．依据计算

出的分析值 q_j 和 0 之间的距离，确定出是否嵌入了数字水印.

另外，使用该计算得到的测试值 q_j 则能计算作为数字水印而被嵌入的信息. 当用等式（3）嵌入数字水印时，如果 q_j 为正，则确定位元为“1”，或者如果 q_j 为负，则位元为“0”.

如同用于提取数字水印的原理，参考现有技术的内容.

前述的数字水印提取处理，用于实现所有的像素，也包括那些由于其不满足等式（4）（或等式(4′)）给定的条件通过数字水印形成单元 2203 而没有嵌入数字水印的像素. 由于不满足等式（4）（或等式(4′)）给定的条件的像素数比整个图像的像素总数小，在提取数字水印时，即使包括上述的那些像素，也能正确的提取数字水印.

以这种方式提取的数字水印为由溢出信息 R 和附加信息 Inf 组成的代码序列 w，而且代码序列 w 被分割为溢出信息 R 和附加信息 Inf. 之后，数字水印消除单元执行:

If i c R then $I''=I'$

else $I''_{j,i}=I'_{j,i}-c_j \times a_i \times x_i$ (5)

其中 $I''_{i,j}$ 为恢复的图像数据，$I'_{i,j}$ 为输入到图像恢复装置的图像数据，如果由数字水印提取单元提取的附加信息 Inf 中的位元为 1，则 C_j 为常数+1，或者如果该位元为“0”，则 C_j 为常数-1，而 a_i 和 x_i 与等式（3）中的意义相同. 也就是，如果 i 不包括在溢出信息 R 中，则执行与等式（3）相反的处理；如果 i 包括在溢出信息 R 中，则没有执行任何处理.

当通过前述的处理正确提取出代码序列 w 时，该恢复的图像 I″ 与原始图像 I 相同.

[实际装置的说明]

对于本领域技术人员来说，通过执行前述处理的程序，容易实现用于嵌入数字水印的装置和用于提取该嵌入的数字水印并恢复原始图像的装置.

图 8 示出了该装置的实用结构，以及与数字水印的嵌入相关联的过程（程序），并且在介绍图 8 之后，介绍恢复处理（程序）.

参照图 8，主机 2101 例如为一广泛使用的个人电脑.

下面将要介绍的，在主机 2101 内部的相应单元经过总线 2107 连接起来以交换不同的数据.

参照图 8，标号 2102 代表一监视器（显示设备），而 2103 代表一 CPU，它能控制相应的内部单元的操作或执行内部存储的程序。标号 2104 表示一存储引导程序和 BIOS 的 ROM。标号 2105 代表在由 CPU 执行一处理时，暂时存储程序或将要处理的图像数据的 RAM。标号 2106 代表一硬盘，它能预先存储将要传递到 RAM 或类似单元的程序（OS 和图像处理程序）和图像数据，并能保存处理过的图像数据。

标号 2108 表示一 CD 驱动装置：它能装入存储在作为一种外置的存储介质 CD(CD-R)上的数据，或者将数据写在 CD-R 上。标号 2109 表示一与 CD 驱动装置 2108 类似的且能从 FD 装入数据或将数据写入 FD 的 FD 驱动装置。标号 2110 表示一与 CD 驱动装置 2108 相似的且能从 DVD 装入数据或将数据写入 DVD 的 DVD 驱动装置。注意当 CD、FD、DVD 或类似物存储图像编辑程序或打印机驱动程序时，这样的程序在需要时被装入 HD 106 并传送到 RAM 105。标号 2113 代表一与键盘 2111 和鼠标 2112 相连的并能接收从其输入的指令的接口（I/F）。标号 2114 代表用于连接至网络例如互联网的通信接口。

嵌入有数字水印的图像的输出终端可能是类似 HD、FD 的存储介质，或者是网络上的文件服务器。也同样应用于接收嵌入有数字水印的信息的介质。

当前述的装置用做数字水印嵌入装置时，则按照图 18 的流程执行。注意下面将要介绍的同该流程关联的程序被安装在 HD 2106 上。同时，将要嵌入的信息从例如键盘输入。或者也可使用预先存储在 HD 2106、ROM 21047、RAM 2105 或类似物上的信息。

在步骤 S101 中，输出将要嵌入数字水印的图象数据。输入源没有特别的限定，图象数据可以是从网络下载的，或是使用图象扫描仪之类的装置输入的。在步骤 S102 中，检测来自于输入的图象数据的所有溢出像素的位置，并且作为溢出信息 R 保存在 RAM 2105 中。预先输入的附加信息 Inf 和溢出信息 R 被组合编码（通过可逆编码）来产生将要在应用时嵌入的信息 w，且该信息暂时保存在 RAM 2105 中。

输入的图象数据中的每个像素被选做要研究的像素，并校验所要研究的像素是否包含在溢出信息 R 中。如果该像素 的位置不包括在溢出信息 R 中，则从信息 w 中提取 1 个比特，并且执行与该比特状态相一致的数字水印形成过程。

另外，如果所研究的像素位置包括在溢出信息 R 中，则没有执行任何数字

水印形成过程。

这个过程重复于所有的位信息和像素（步骤 S106 和 S107）。一旦完成用于所有的位信息和所有的像素的处理，则嵌入有数字水印的图象数据被输出到 RAM 2105 或 HD 2106（步骤 S108）。

如果信息 w 的所有比特的嵌入是在所有像素的嵌入完成之前完成的，可能嵌入假程序信息或信息 w 可能被重复嵌入。

其结果，嵌入之后的图象信息 I′ 产生在 RAM 上。该图象 I′ 作为文件最后被存储在例如 HD 或类似介质上。之后，该图象 I′ 可能经过网络传递或存储在例如可拆装的介质上。

下面将用图 19 来解释用于提取数字水印和恢复原始图象的过程。

嵌入有数字水印的图象数据 I′ 输入到 RAM 2105（步骤 S1201）。如上所述的，输入源并未受到特定限制。之后，在步骤 S1202 中，从嵌入图像 I′ 中提取出数字水印信息。数字水印的提取原理与上面介绍的相同。

在步骤 S1203 中，该提取的信息被译码以将信息 w（=溢出信息 R+嵌入的信息 Inf）存储在 RAM 2105 中，这样就完成了提取处理。注意嵌入的信息 Inf 可能显示在显示屏上。

在步骤 S1204 中，图象数据中的每个像素都被选做为要研究的像素，并校验所研究的像素位置是否包含于溢出信息 R 中。

如果所研究的像素不包含在溢出信息 R 中，则在步骤 S1205 中执行数字水印消除处理。

另外，如果所研究的像素包含在溢出信息 R 中，则跳过用于该像素的数字水印消除处理，并且利用所输入的图象数据的像素值。

所执行的这种处理用于所有的像素（步骤 S1206）。一旦完成用于所有像素的处理，则通过消除数字水印，重现原始图象。在需要时，该结果（原始图象数据）被输出到 RAM 2105、HD 2106 或类似的装置，并且将之显示。

在上面的实施例中，溢出像素数比整个图象的像素总数相对小的多。即，溢出信息 R 的信息容量相对较小，并且随数字水印一起相对稳定的嵌入信息 R。例如，这种情况适用于类似照片之类的自然图象。

另外，随图象数据的类型，溢出信息 R 可以有大信息容量。例如，当数字水印嵌入亮度值时，当图象的整个亮度或高或低时，溢出信息 R 变大。

当溢出信息 R 的容量变得很大时，包含溢出信息 R 的代码序列 W 的信息容量也变得很大，并且该代码序列 w 不能作为数字水印被嵌入。因此，溢出信息 R 的信息容量最好减至最小。下面将介绍用于减少溢出信息 R 的容量的过程的例子。

图 12 示出了数字水印形成装置的内部结构。与图 9 所示装置的不同之处在于增加了校正单元 2501 和用于处理信息的编码单元 2503。由于其它操作同图 9 所示的相同，由此将其省去。

图象数据 I 被输入到校正单元 2501，该单元执行一校正过程以减少溢出信息 R 的信息容量，并输出校正后的图象数据 I′′′ 和表示执行校正类型的校正信息 C。

校正的过程是用于减少溢出信息 R 的信息容量的过程。例如，当整个图象的亮度为高时，则执行从所有的像素值减去一给定的量（d）的过程。在这种情况下，表示“从整个图象的像素值中减去给定的量（d）”的信息作为校正信息 C 被输出。

另外，除了溢出信息 R 和附加信息 Inf 之外，编码单元 2503 还对校正信息 C 编码。如图 20 所示，编码后的代码序列 w 包括校正信息 C、溢出信息 R 和附加信息 Inf。

通过前述的过程嵌入数字水印。下面将介绍图象恢复装置。

图 13 示出了本实施例中的图象恢复装置的内部结构。同图 10 所示装置的不同之处在于增加了反向校正单元 2604 和处理存储信息的译码单元 2602。由于其它操作同图 13 和 10 中的相同，则将其省略。

译码单元 2602 接收由数字水印提取单元 2601 提取的代码序列 w，并对该输入的序列 w 进行译码以获取附加信息 Inf、溢出信息 R 和校正信息 C，并将它们输出。

反向校正单元 2604 接收通过数字水印消除单元从中将数字水印消除的图象数据 I′′′ 和由译码单元 2602 对其进行译码的校正信息 C，并且该单元执行同校正单元 2503 执行的过程相反的过程，并输出校正后的图象数据 I。例如，如果表示“从整个图象的像素值减去给定的量（d）”的信息作为校正信息被输入，则校正单元 2604 执行这样的处理：将一给定量（d）加到整个图象的像素值。

通过上面的过程，能从输入到图象恢复装置的图象数据I′完美的再现数字水印形成之前的图象数据I.

下面将举例介绍校正信息C的确定方法.

检测将嵌入数字水印的图象的亮度分布．例如，如果亮度值的出现率比在低亮度区的大，则产生校正以变换发光率至低亮度区．相反地，如果低度值的出现率比在高亮度区的大，则产生校正以变换发光率至高亮度区.

在一些情况下，可能进行下述处理．为了容易理解，下面将分析使用图象扫描仪（每像素8比特）来读取印有文本的纸张且该读取的图象作为图象I而被使用的情况.

一般的，如图21所示，当读取印有文本的文件（二元图象）且用亮度值来表示相应的像素时，像素的分布集中在最高和最低亮度值部分，且在它们之间几乎没有像素.

在这种情况下，如果所有的像素值加上或减去一给定的值，则在高或低亮度侧发生溢出．因此，执行以下处理.

由于低亮度范围分布在亮度值0至a之间，则找出与0出现率相一致且满足等式(4)(或等式(4′))的中间亮度值，且用找出的亮度值来代替低亮度值.例如，如果找出50到50+a之间的亮度值，则0至a的亮度值转换为50至50+a之间的值（0转换为50，1转换为51，…）．对于高亮度范围也进行了相似的处理．即高亮度范围变换为较低的亮度范围.

作为上述过程的结果，尤其在类似于文本的二元图象的情况下，如果校正信息C表明亮度值0至a和亮度区b至255之间的转换值，则能完美的恢复原始图象．在上面的叙述中，图象用亮度分量表示，然而，本发明不局限于此，图象也可用其它类似色度的分量表示.

如上所述的，按照上面的实施例，当溢出像素（数字数据的组成元素）没进行嵌入处理且作为数字水印的信息嵌入到任何没有溢出的像素时，能完美的恢复原始图象数据.

注意如上所述的，本发明能通过运行在计算机上的程序来实现．因此，本发明包括一计算机程序．由于本发明能通过给计算机提供程序来实现，则用于将程序代码输给计算机的装置即用于存储程序代码的存储介质也在本发明范围内.

类似这样的存储程序代码的存储介质，例如，可以使用软盘、硬盘、光盘、磁光盘、CD-ROM、磁带、永久性存储器卡、ROM或类似物。

可以独自控制与提供的程序代码相匹配的不同设备的计算机，不但可以通过这样的计算机来实现上述实施例的功能时，而且在协同运行在计算机上的程序代码和OS（操作系统）或其它软件来实现该实施例的功能时，这样的程序代码都包括在本发明的范围内。

另外本发明的范围还包括这样一种情况：提供的程序代码存储于安装在计算机主板上的存储器或与计算机相连的功能扩充装置，安装于该功能扩充板或装置上的CPU在程序代码指令的基础上执行一些或所有的有效过程，并通过这些过程实现本实施例。

如上所述的，依据本发明，当鉴别信息与数字信息不可分开的设置时，总能检测到信息是否被篡改，而且只要原始数据不被篡改总能将其恢复。

可以嵌入数字水印，而且嵌入有数字水印的原始数字数据能被再现。

因为可以在不脱离本发明精神和范围的情况下，产生许多不同的实施例，所以可以理解本发明不局限于所限定的具体实施例而是由所附的权利要求来限定。

说 明 书 附 图

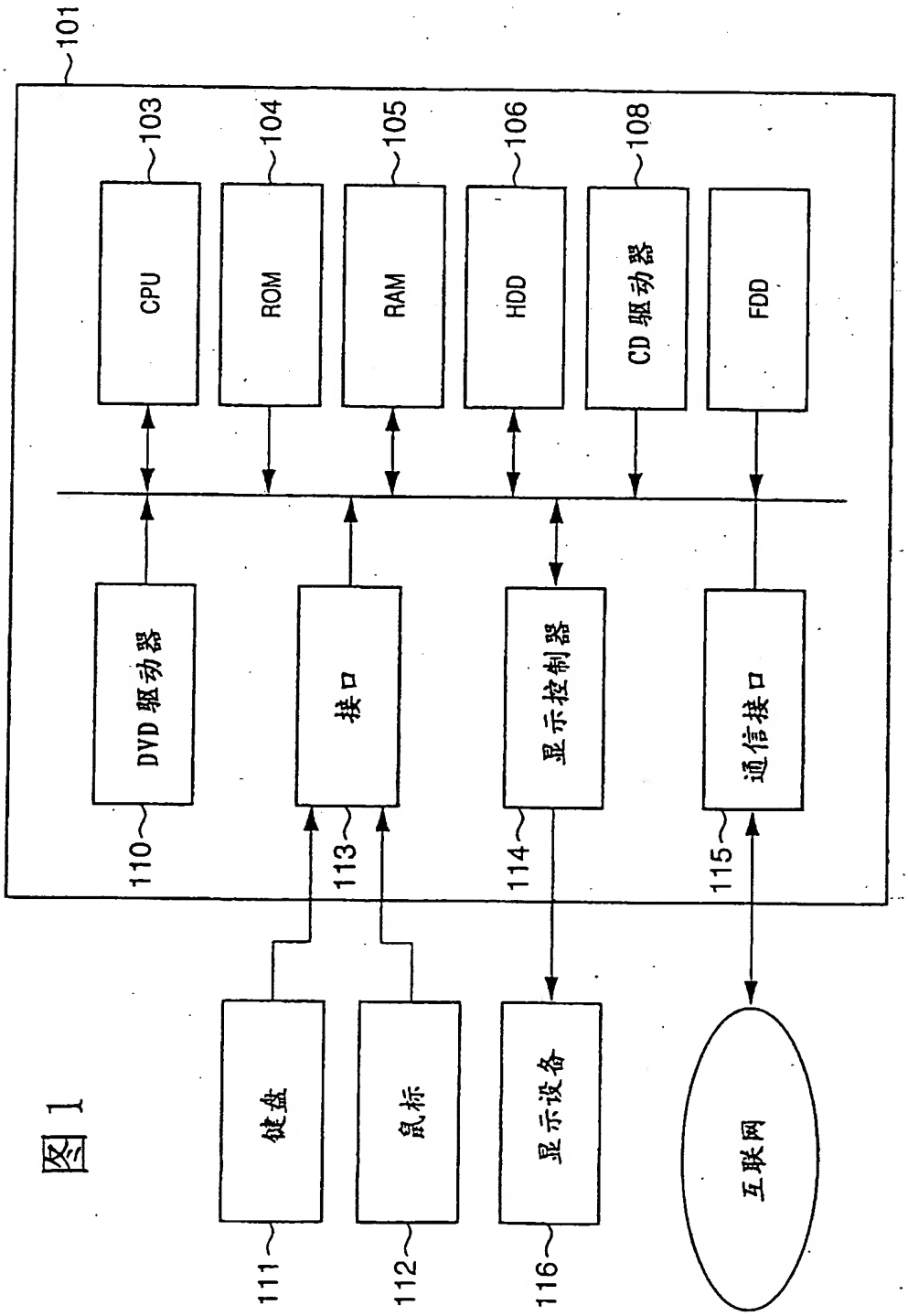

101
CPU
103
ROM
104
RAM
105
HDD
106
CD 驱动器
108
FDD
DVD 驱动器
110
接口
113
显示控制器
114
通信接口
115
键盘
111
鼠标
112
显示设备
116
互联网

图 1

图 2

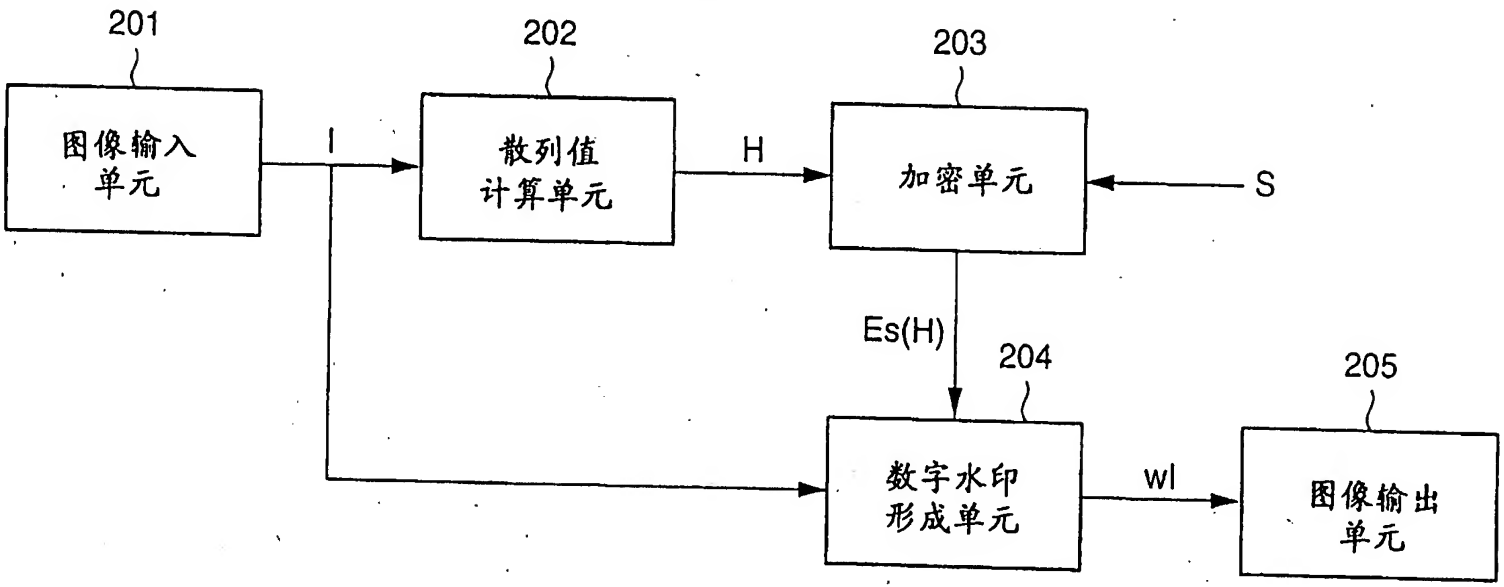

201
图像输入
单元
I
202
散列值
计算单元
H
203
加密单元
S
Es(H)
204
数字水印
形成单元
wI
205
图像输出
单元

图 3

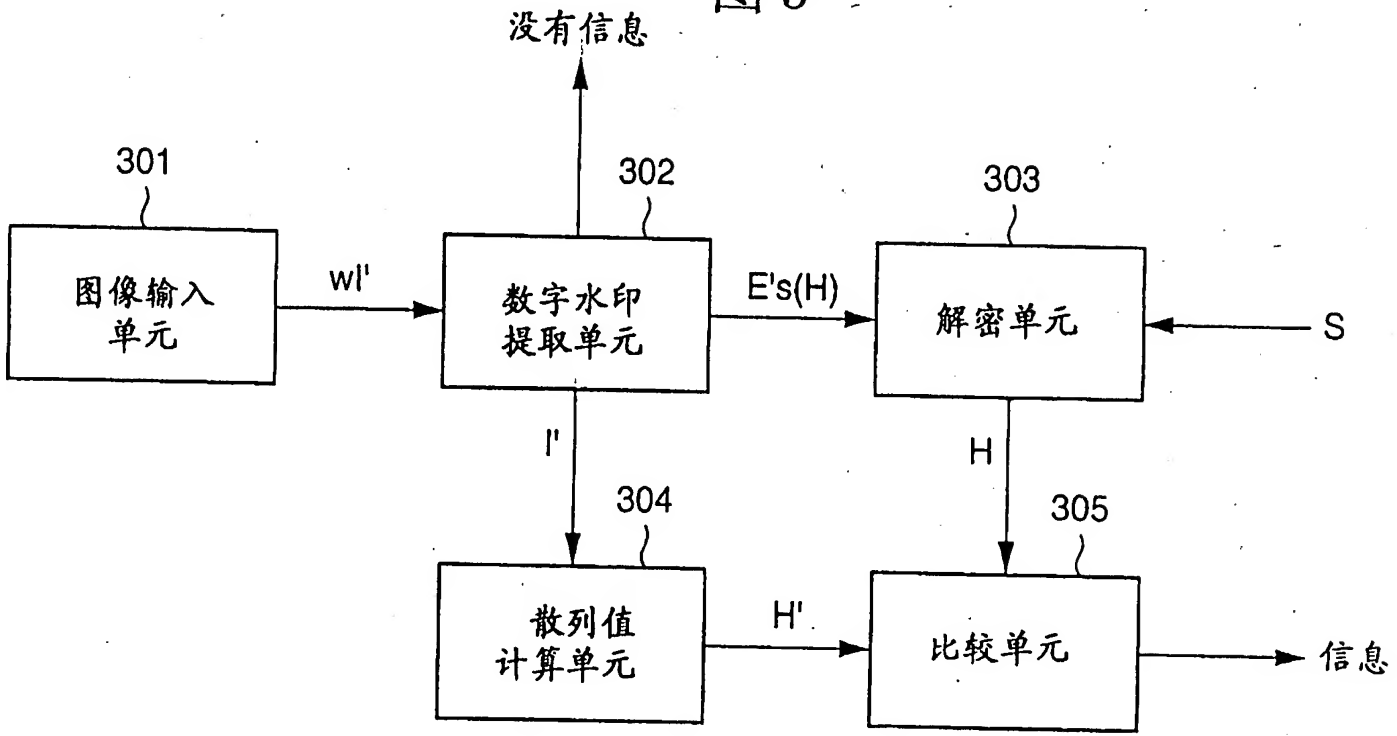
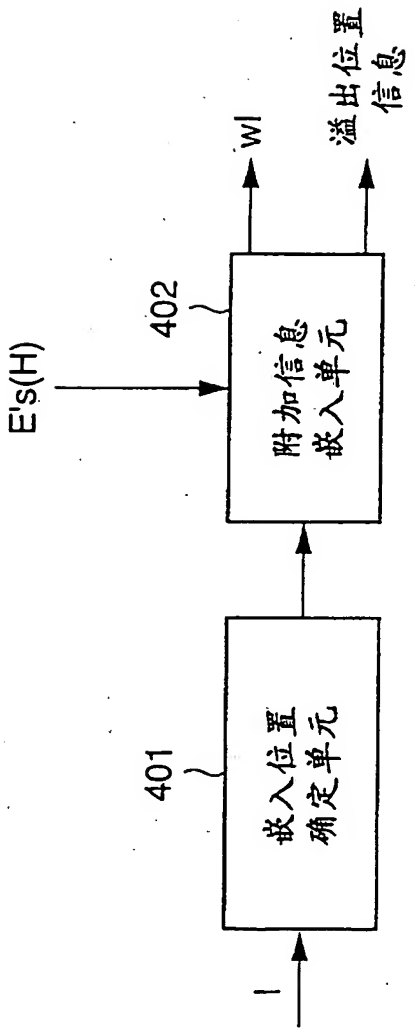

没有信息
301
302
303
图像输入
单元
wI'
数字水印
提取单元
E's(H)
解密单元
S
I'
H
304
305
散列值
计算单元
H'
比较单元
信息

图 4



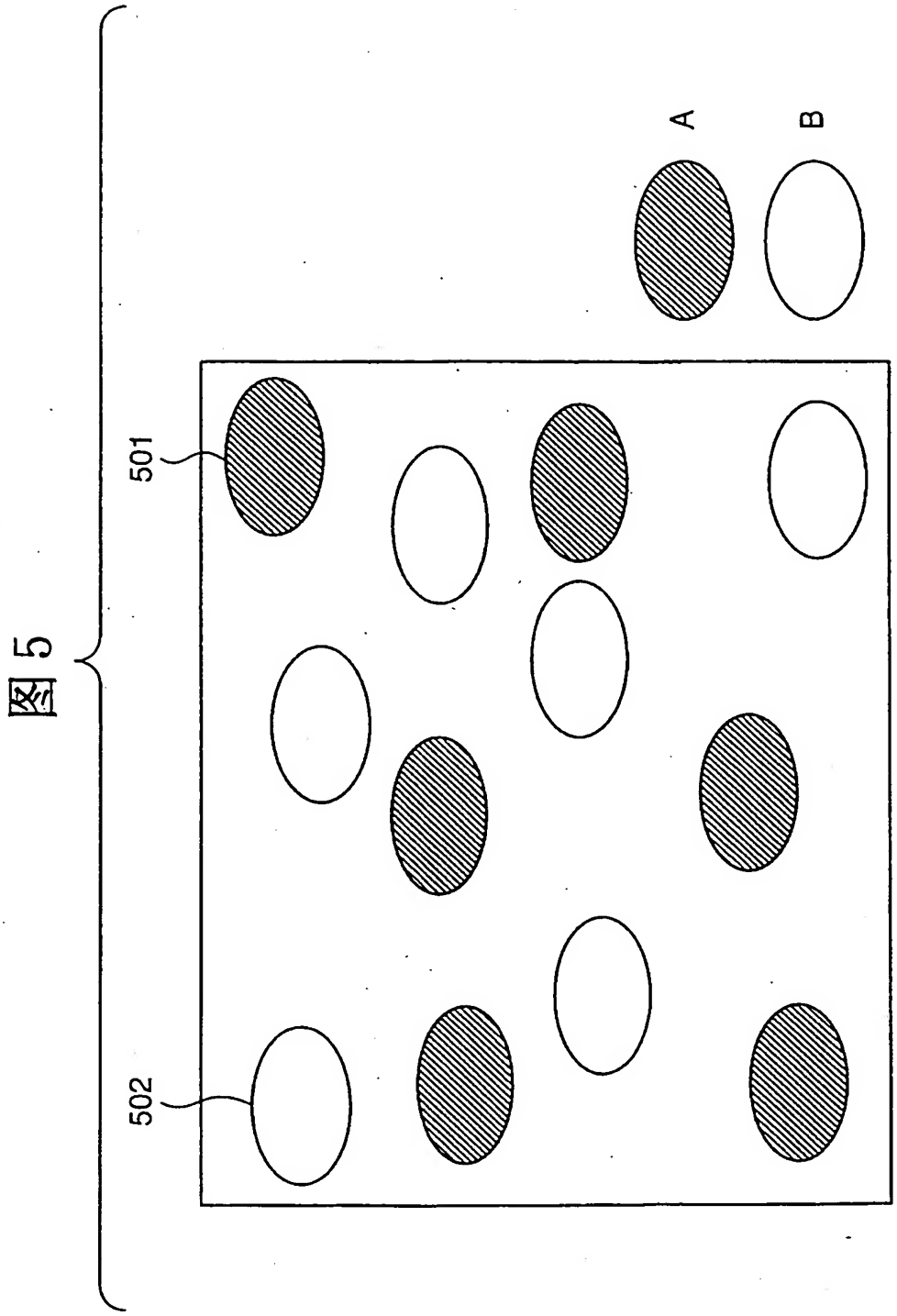


图 5

图 6

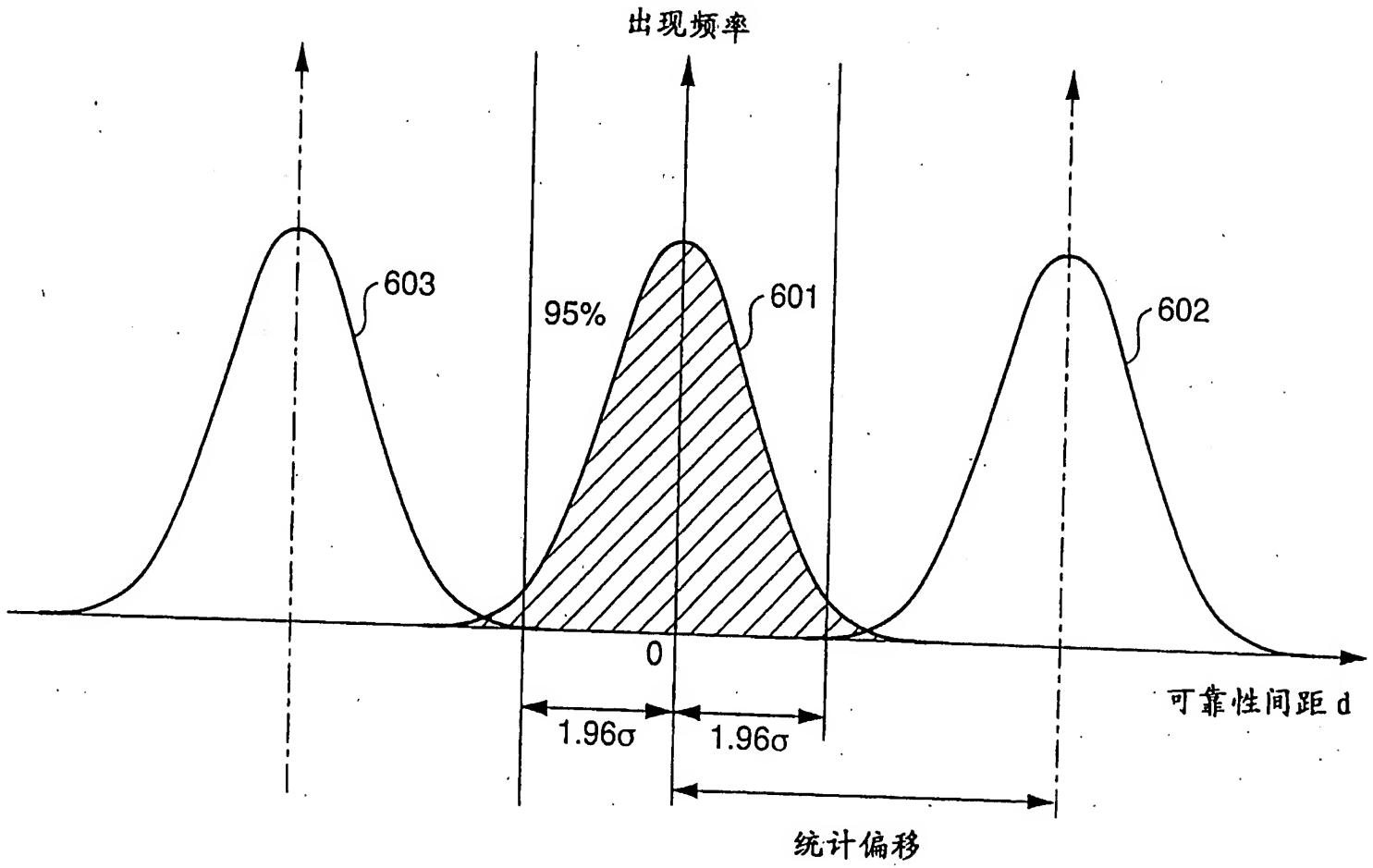


图 7

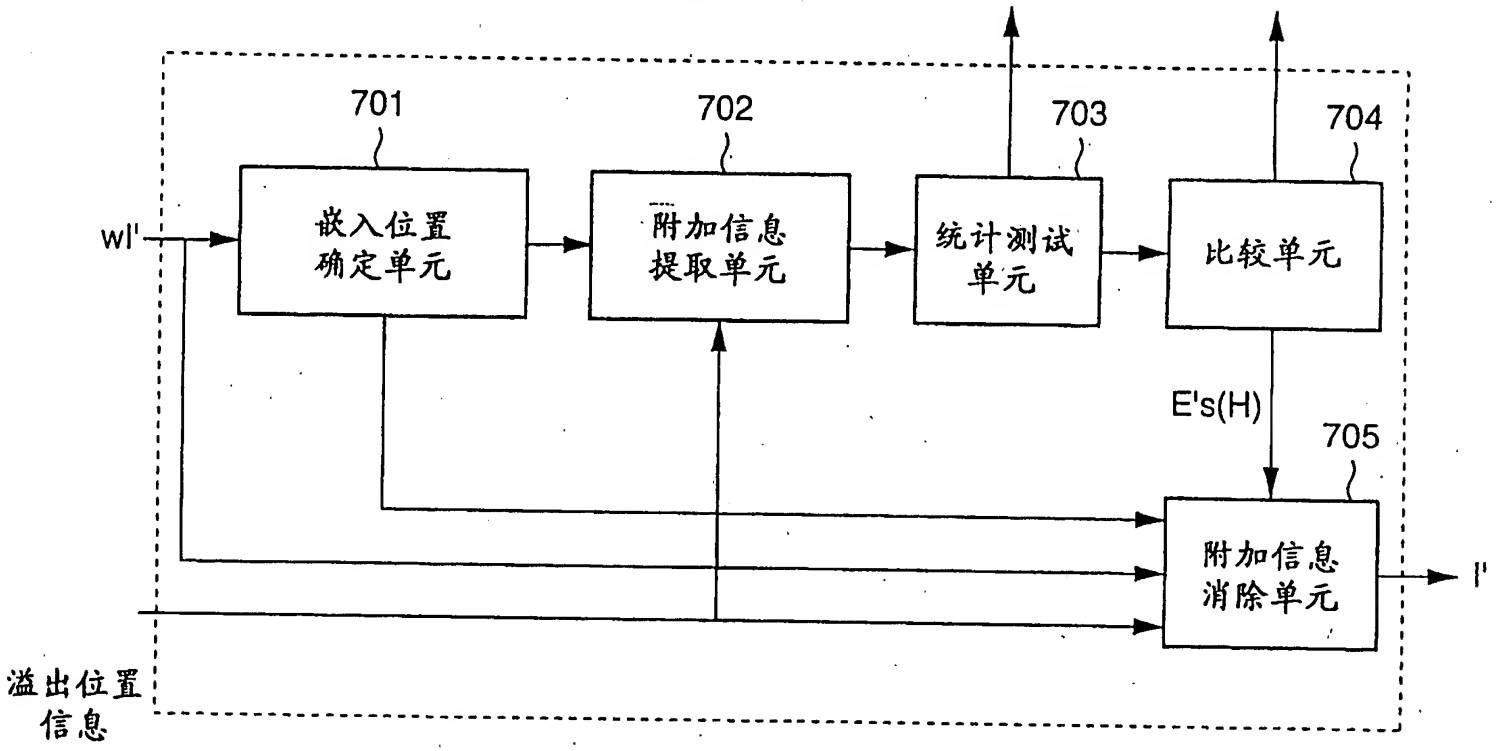

701
702
703
704
wI'
嵌入位置
确定单元
附加信息
提取单元
统计测试
单元
比较单元
E's(H)
705
附加信息
消除单元
I'
溢出位置
信息

图 8

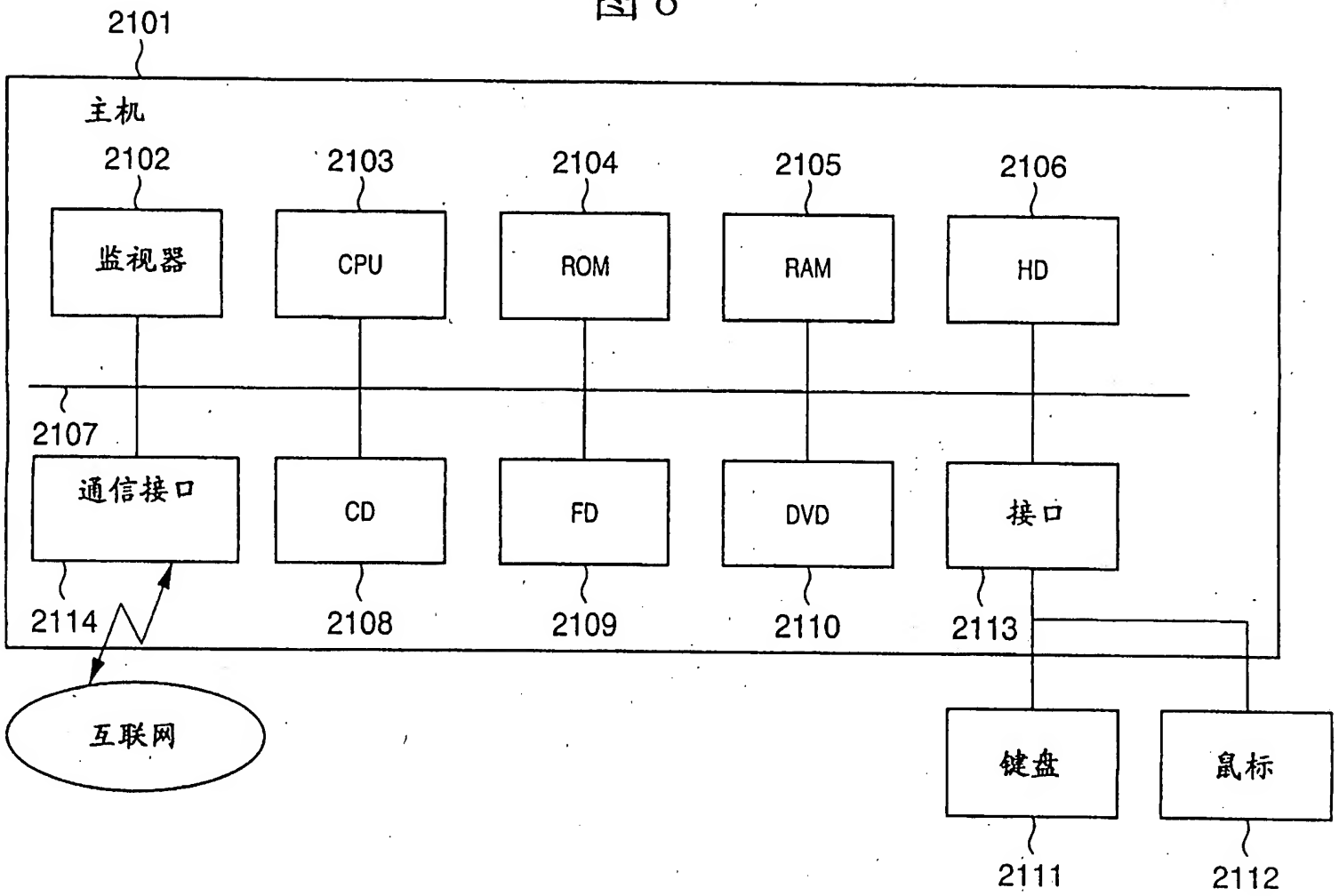

2101
主机
2102
2103
2104
2105
2106
监视器
CPU
ROM
RAM
HD
2107
通信接口
CD
FD
DVD
接口
2114
2108
2109
2110
2113
互联网
键盘
鼠标
2111
2112

图 9

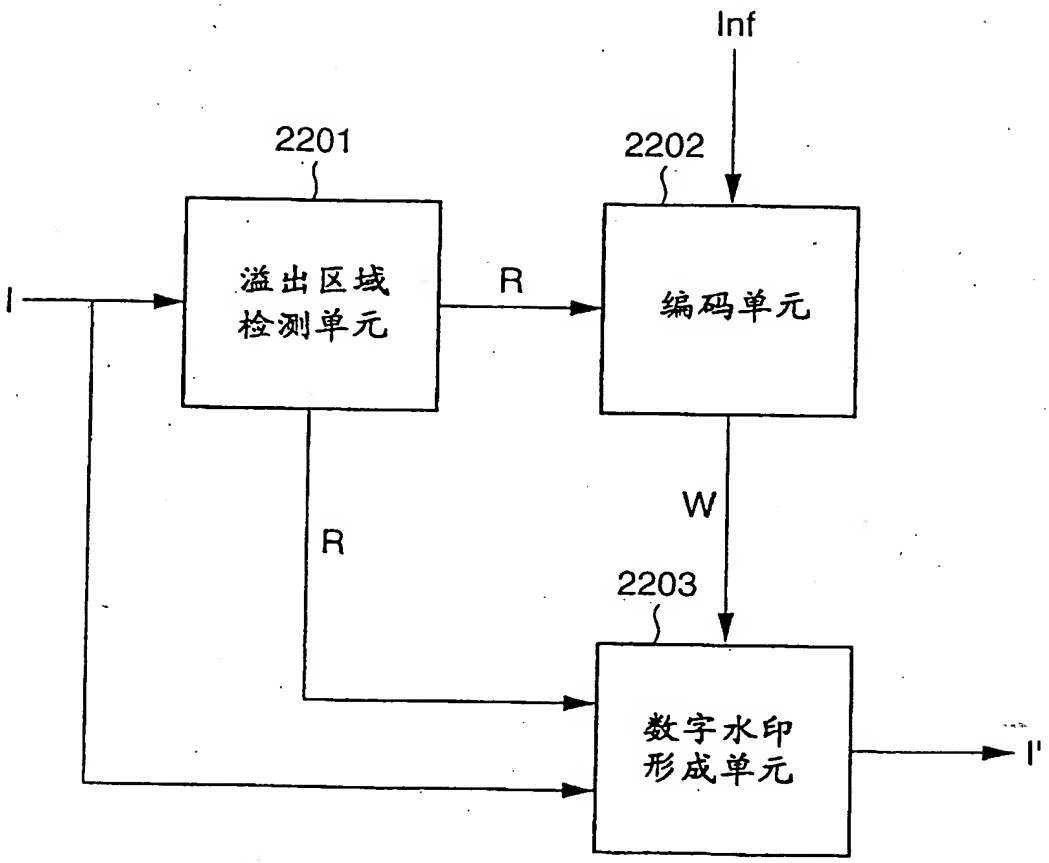


图 10

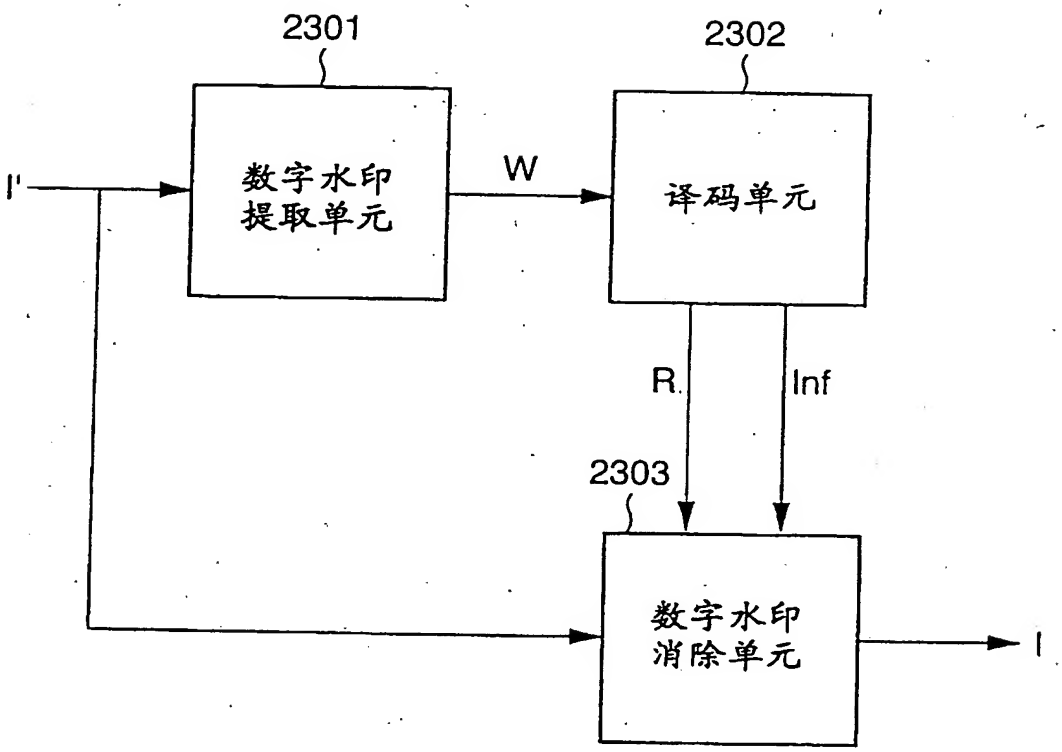


图 11

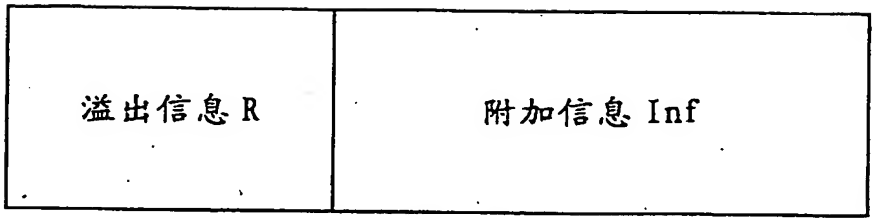


图 12

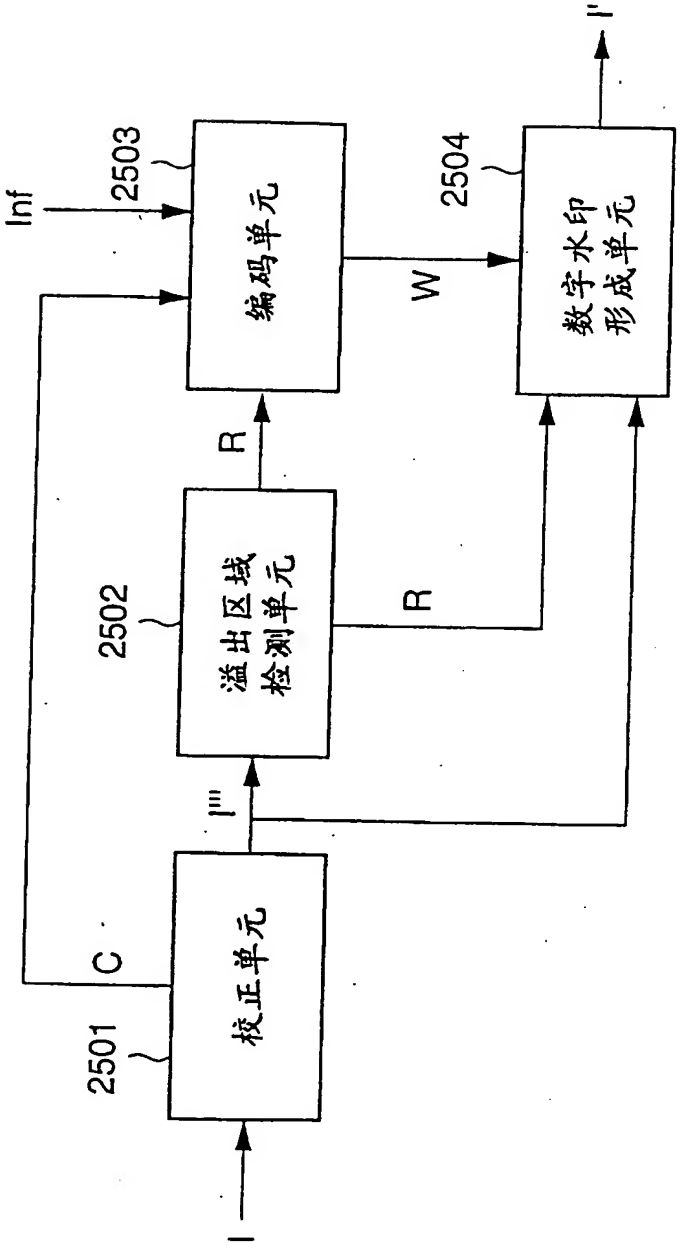

I
2501
校正单元
C
I'''
2502
溢出区域检测单元
R
R
Inf
2503
编码单元
W
2504
数字水印形成单元
I'

图 13

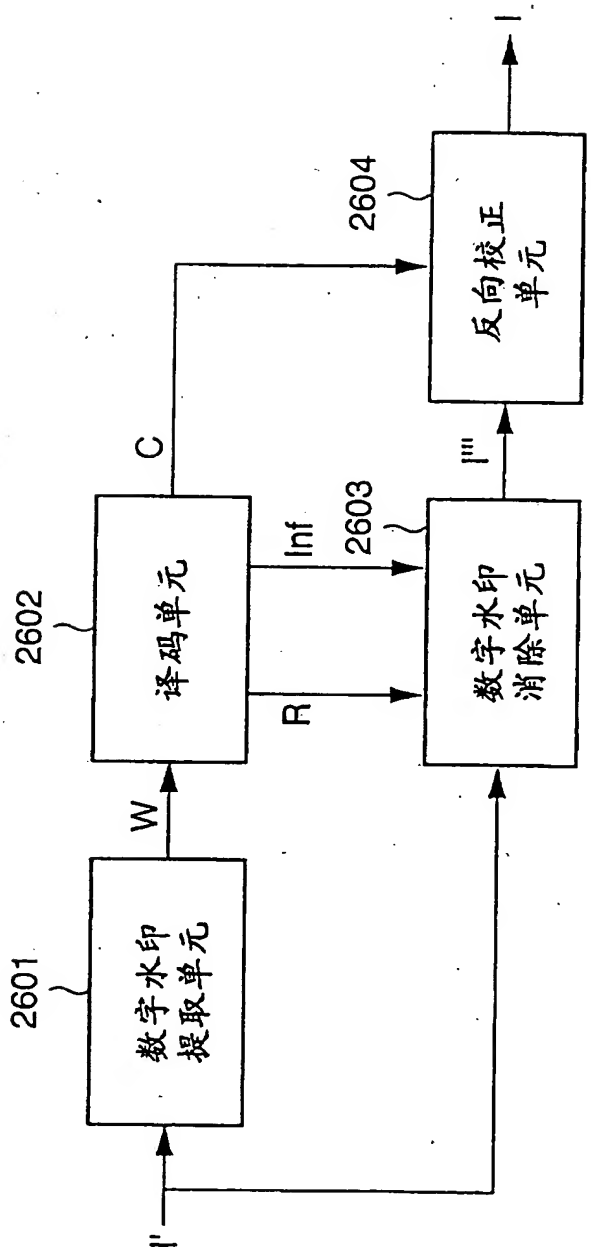

I'
2601
数字水印
提取单元
W
2602
译码单元
C
Inf
R
2603
数字水印
消除单元
I'''
2604
反向校正
单元
I

图 14

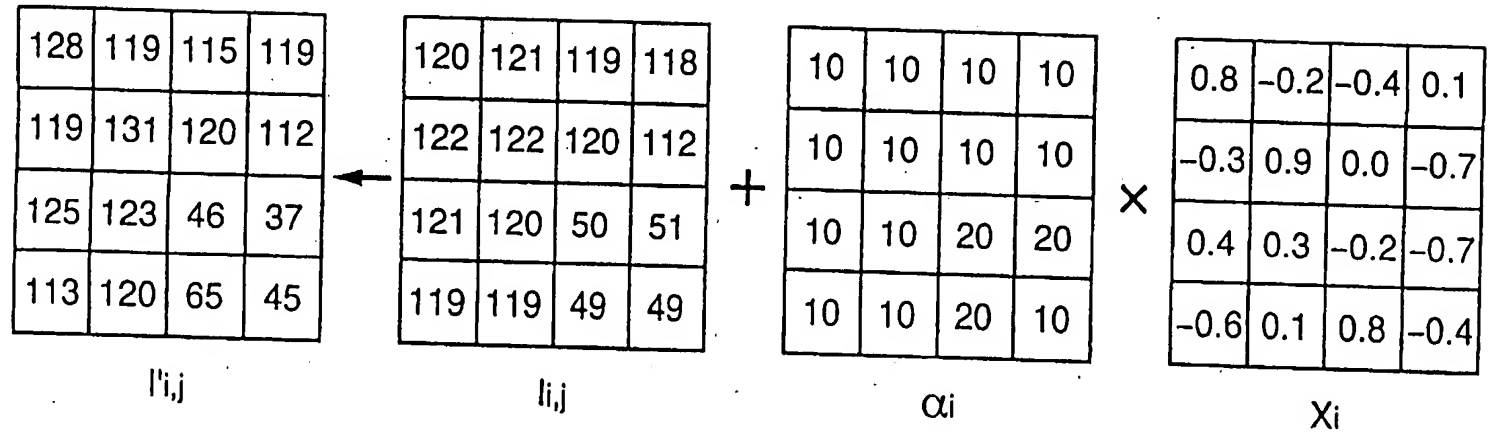

128 119 115 119
119 131 120 112
125 123 46 37
113 120 65 45
I'i,j
120 121 119 118
122 122 120 112
121 120 50 51
119 119 49 49
Ii,j
+
10 10 10 10
10 10 10 10
10 10 20 20
10 10 20 10
αi
×
0.8 -0.2 -0.4 0.1
-0.3 0.9 0.0 -0.7
0.4 0.3 -0.2 -0.7
-0.6 0.1 0.8 -0.4
Xi

图 15

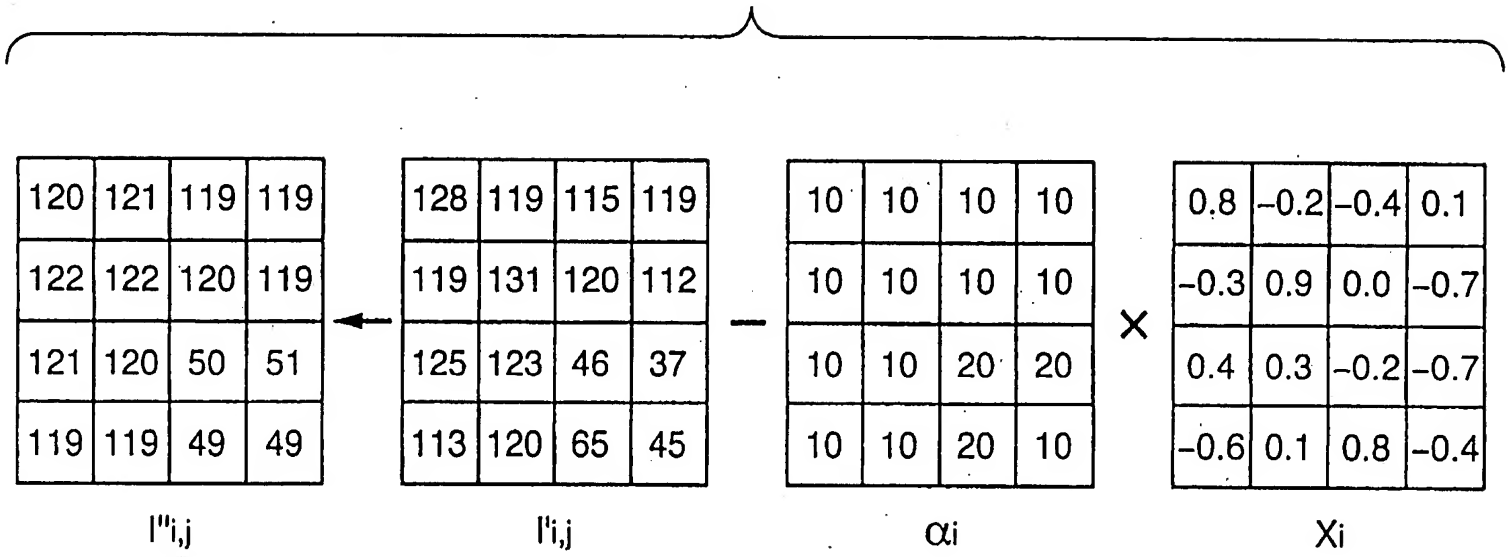

120 121 119 119
122 122 120 119
121 120 50 51
119 119 49 49
I''i,j
128 119 115 119
119 131 120 112
125 123 46 37
113 120 65 45
I'i,j
10 10 10 10
10 10 10 10
10 10 20 20
10 10 20 10
αi
0.8 -0.2 -0.4 0.1
-0.3 0.9 0.0 -0.7
0.4 0.3 -0.2 -0.7
-0.6 0.1 0.8 -0.4
Xi

图 16

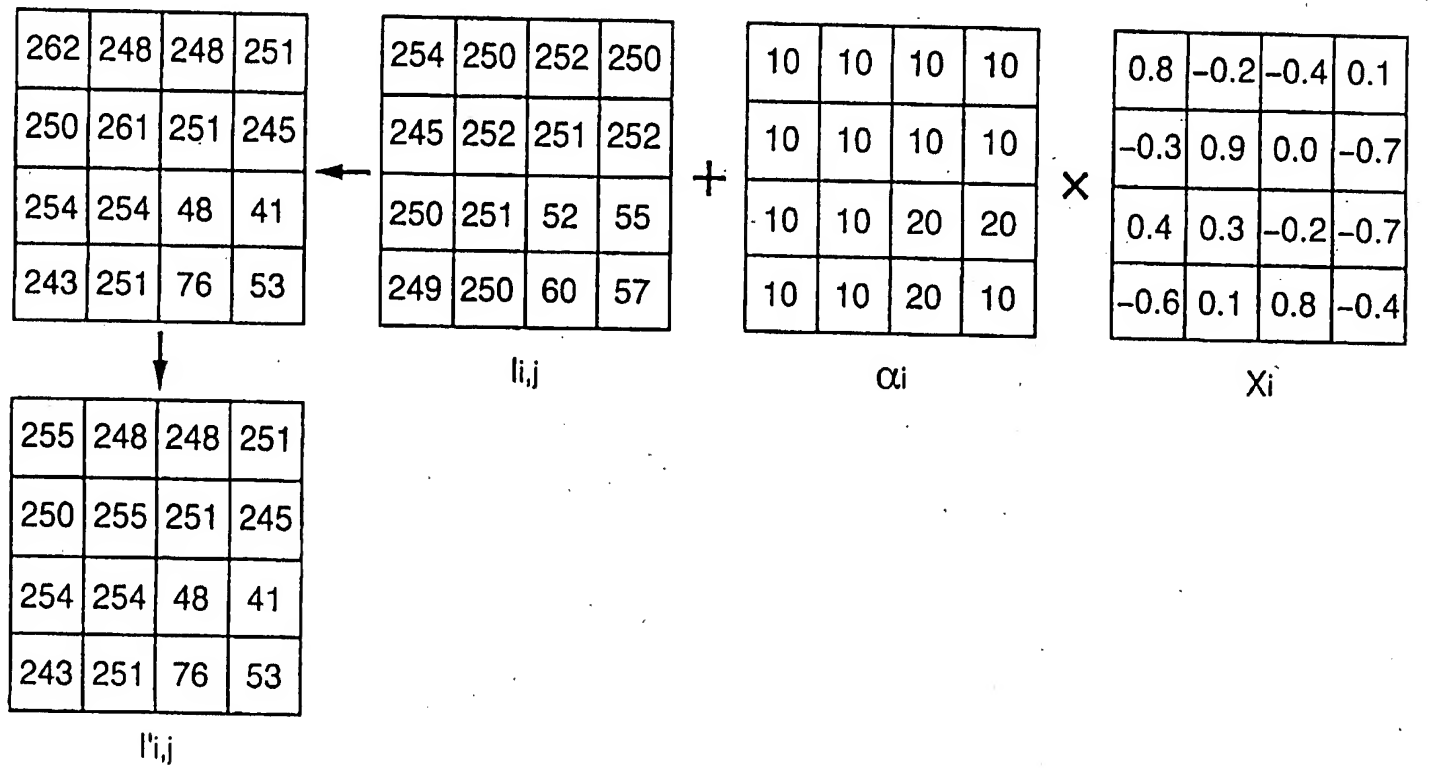

262 248 248 251
250 261 251 245
254 254 48 41
243 251 76 53
254 250 252 250
245 252 251 252
250 251 52 55
249 250 60 57
10 10 10 10
10 10 10 10
10 10 20 20
10 10 20 10
0.8 -0.2 -0.4 0.1
-0.3 0.9 0.0 -0.7
0.4 0.3 -0.2 -0.7
-0.6 0.1 0.8 -0.4
255 248 248 251
250 255 251 245
254 254 48 41
243 251 76 53
I'i,j
Ii,j
αi
Xi

图 17

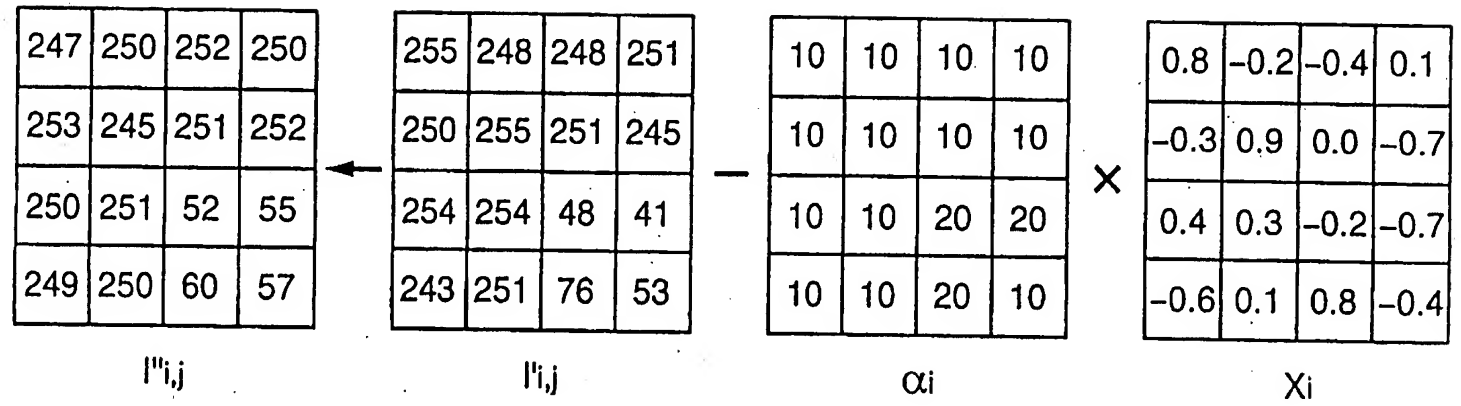

247 250 252 250
253 245 251 252
250 251 52 55
249 250 60 57
I''i,j
255 248 248 251
250 255 251 245
254 254 48 41
243 251 76 53
I'i,j
10 10 10 10
10 10 10 10
10 10 20 20
10 10 20 10
αi
0.8 -0.2 -0.4 0.1
-0.3 0.9 0.0 -0.7
0.4 0.3 -0.2 -0.7
-0.6 0.1 0.8 -0.4
Xi

图18

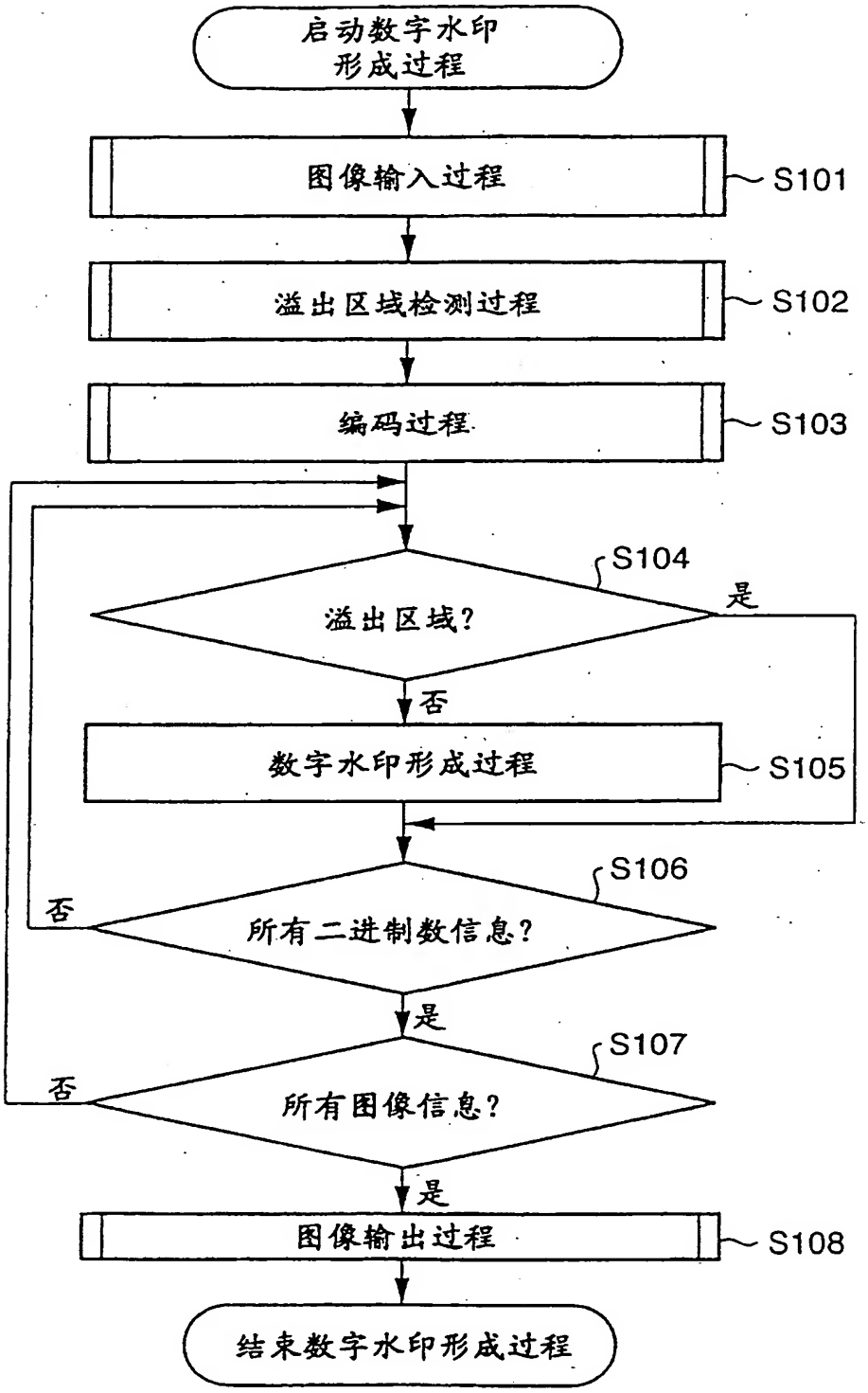

启动数字水印形成过程
图像输入过程
S101
溢出区域检测过程
S102
编码过程
S103
S104
溢出区域?
是
否
数字水印形成过程
S105
S106
所有二进制数信息?
否
是
S107
所有图像信息?
否
是
图像输出过程
S108
结束数字水印形成过程

图19

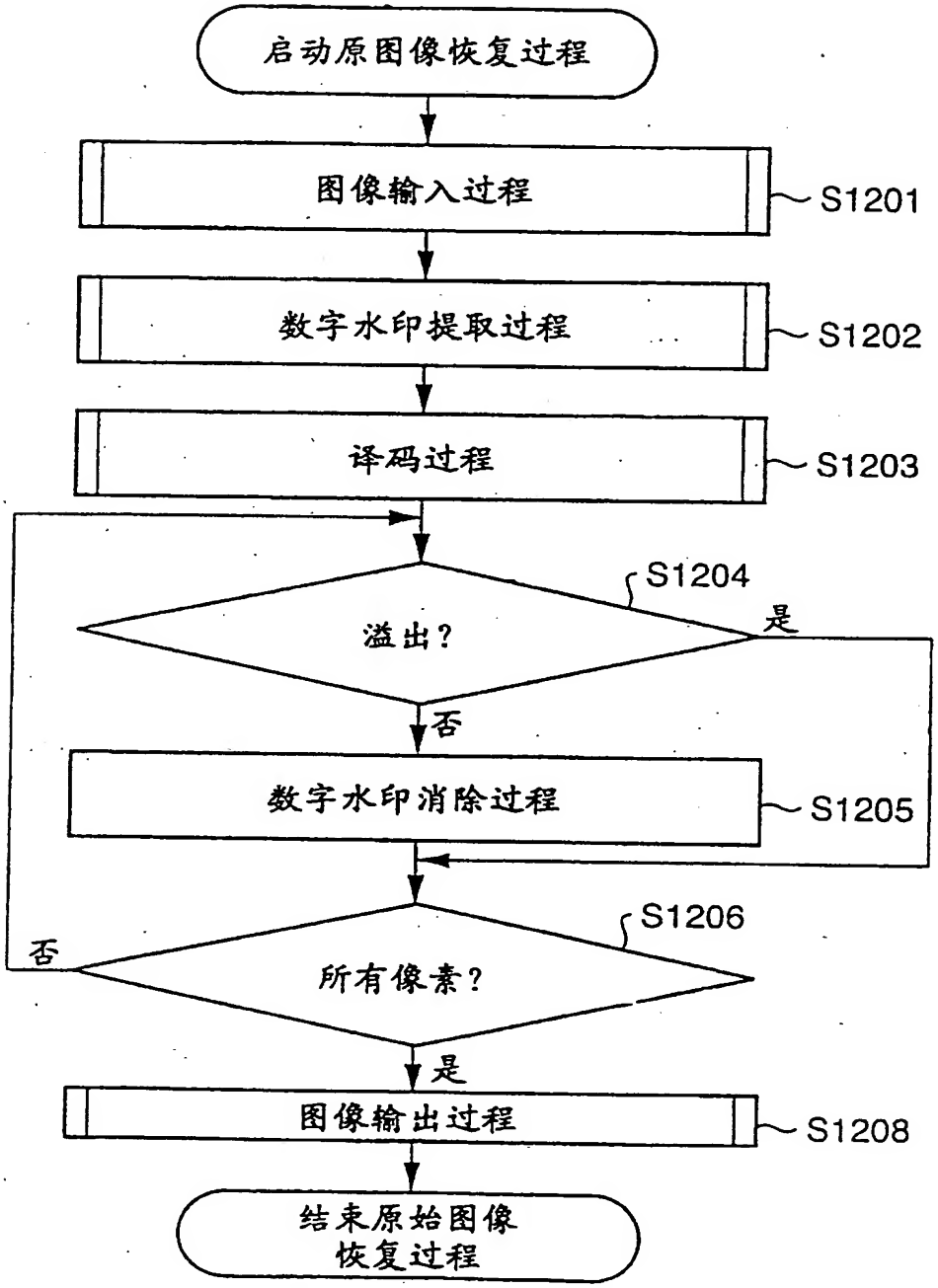
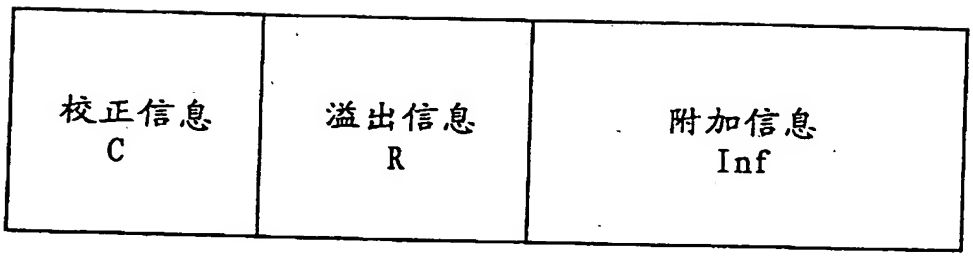

启动原图像恢复过程
图像输入过程
S1201
数字水印提取过程
S1202
译码过程
S1203
S1204
溢出？
是
否
数字水印消除过程
S1205
S1206
所有像素？
否
是
图像输出过程
S1208
结束原始图像
恢复过程

图 20



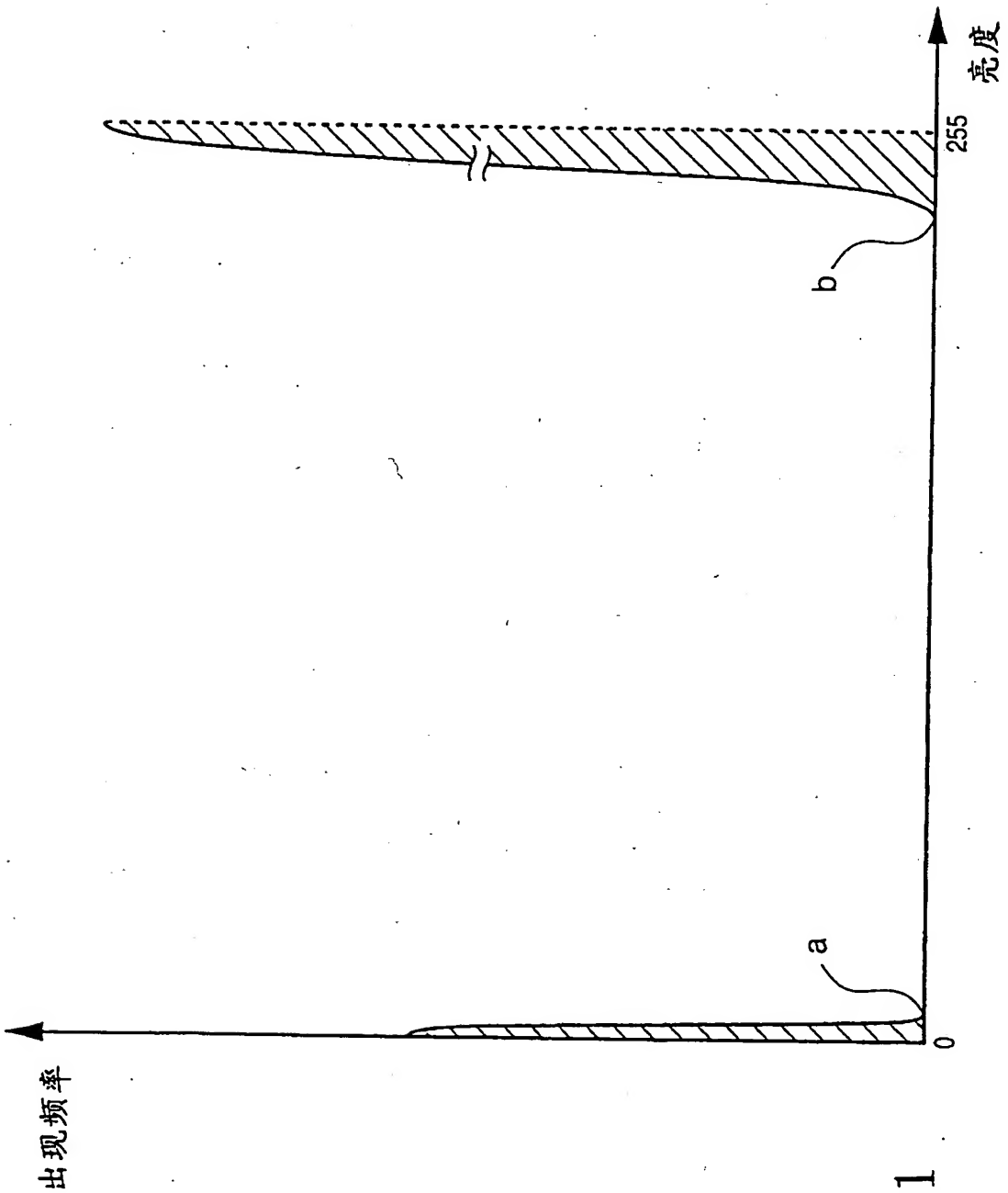


图 21